



Report to the Chairman, Subcommittee on
Federal Financial Management, Government
Information, Federal Services, and International
Security, Committee on Homeland Security and
Governmental Affairs, U.S. Senate

September 2010

CONTRACTOR INTEGRITY

Stronger Safeguards Needed for Contractor Access to Sensitive Information



GAO

Accountability * Integrity * Reliability

Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE SEP 2010		2. REPORT TYPE		3. DATES COVERED 00-00-2010 to 00-00-2010	
4. TITLE AND SUBTITLE Contractor Integrity: Stronger Safeguards Needed for Contractor Access to Sensitive Information				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) U.S. Government Accountability Office, 441 G Street NW, Washington, DC, 20548				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT Same as Report (SAR)	18. NUMBER OF PAGES 72	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			



Highlights of [GAO-10-693](#), a report to the Chairman, Subcommittee on Federal Financial Management, Government Information, Federal Services, and International Security, Committee on Homeland Security and Governmental Affairs, U.S. Senate

Why GAO Did This Study

In performing agency tasks, contractor employees often require access to sensitive information that must be protected from unauthorized disclosure or misuse. This report assesses the (1) extent to which agency guidance and contracts contain safeguards for contractor access to sensitive information, and (2) adequacy of governmentwide guidance on how agencies are to safeguard sensitive information to which contractors may have access. To conduct this work, GAO identified key attributes involving sensitive-information safeguards, analyzed guidance and met with officials at three agencies selected for their extensive reliance on contractor employees, analyzed 42 of their contract actions for services potentially requiring contractor access to sensitive information, and analyzed the Federal Acquisition Regulation (FAR) and pending FAR changes regarding governmentwide guidance on contractor safeguards for access to sensitive information.

What GAO Recommends

GAO recommends that the Office of Federal Procurement Policy (OFPP) ensure pending changes to the FAR address two additional safeguards for contractor access to sensitive information: the use of nondisclosure agreements and prompt notification of unauthorized disclosure or misuse of sensitive information. In oral comments, OFPP agreed with the recommendations. DHS also concurred with the recommendations, while DOD and HHS had no comment.

View [GAO-10-693](#) or [key components](#). For more information, contact John Needham at (202) 512-4841 or needhamjk1@gao.gov.

CONTRACTOR INTEGRITY

Stronger Safeguards Needed for Contractor Access to Sensitive Information

What GAO Found

GAO's analysis of guidance and contract actions at three agencies found areas where sensitive information is not fully safeguarded and thus may remain at risk of unauthorized disclosure or misuse. The Departments of Defense (DOD), Homeland Security (DHS), and Health and Human Services (HHS) have all supplemented the FAR and developed some guidance and standard contract provisions, but the safeguards available in DOD's and HHS's guidance do not always protect all relevant types of sensitive information contractors may access during contract performance (examples of some types of sensitive information contractors may access are listed below). Also, DOD's, DHS's, and HHS's supplemental FAR guidance do not specify contractor responsibilities for prompt notification to the agency if unauthorized disclosure or misuse occurs. Almost half of the 42 contract actions analyzed lacked clauses or provisions that safeguarded against disclosure and inappropriate use of all potential types of sensitive information that contractors might access during contract performance. Additionally, DOD and HHS lack guidance on the use of nondisclosure agreements, while DHS has found that these help accountability by informing contractors of their responsibilities to safeguard confidentiality and appropriate use and the potential consequences they face from violations.

There have been numerous recommendations for improved governmentwide guidance and contract provisions in the FAR, such as prohibiting certain types of contractor personnel from using sensitive information for personal gain. To address some of these areas, regulatory changes are pending to develop standardized approaches and contract clauses in the FAR that agencies could use to safeguard sensitive information, rather than developing such safeguards individually. However, similarly to issues identified in agency guidance, GAO found two key areas the FAR does not yet address. These include (1) agency use of nondisclosure agreements as a condition of contractor access to sensitive information, and (2) the need to establish clear requirements for contractors to promptly notify agencies of unauthorized disclosure and misuse of sensitive information. The ongoing rulemaking process provides an opportunity to address the need for additional FAR guidance in both areas.

Examples of Sensitive Information

Type of information	Examples
Personal	<ul style="list-style-type: none"> Name Social Security number Date and place of birth Patient health and medical information
Business proprietary	<ul style="list-style-type: none"> Trade secrets Manufacturing processes, operations, or techniques Amount or source of any profits, losses, or expenditures.
Agency sensitive	<ul style="list-style-type: none"> Security management information Predecisional planning and budgeting documents Continuity-of-operations information

Source: GAO analysis.

Contents

Letter		1
	Background	4
	Safeguards to Protect Sensitive Information Not Always Available in Agency Guidance or Included in Contract Actions	8
	Efforts Underway to Improve Governmentwide Guidance in the FAR for Contractor Access to Sensitive Information	21
	Conclusions	29
	Recommendations for Executive Action	30
	Agency Comments and Our Evaluation	30
Appendix I	Scope and Methodology	32
Appendix II	Sensitive But Unclassified Markings Identified by President’s Task Force on Controlled Unclassified Information	35
Appendix III	Agency Contract Provisions Containing Contractor Safeguards for Sensitive Information	38
Appendix IV	Contractor Employee Nondisclosure Agreements Used by Agencies	46
Appendix V	Recent FAR Changes to Add Guidance and Contract Provisions for Information Technology (IT) Security	60
Appendix VI	Comments from the Department of Homeland Security	63
Appendix VII	GAO Contact and Staff Acknowledgments	66

Tables

Table 1: Examples of Sensitive Information	6
Table 2: Analysis of Control Practices in Agency FAR Supplements for Safeguarding Sensitive Information Accessed by Contractors	13
Table 3: Analysis of Contract Provisions Establishing Contractor Safeguards for Sensitive Information	17
Table 4: Analysis of Contract Requirements for Nondisclosure Agreements	20
Table 5: FAR Contract Provisions for Safeguarding Certain Types of Sensitive Information	23
Table 6: Status of Pending FAR Cases to Revise Policies and Clauses for Contractor Use and Confidentiality of Sensitive Information	27
Table 7: Selected SBU Markings Currently in Use	36

Figures

Figure 1: HSAR Clause 3052.204-71, Contractor Employee Access	39
Figure 2: DFARS Clause 252.204-7000, Disclosure of Information	43
Figure 3: HHSAR 352.224-70, Confidentiality of Information	44
Figure 4: Source Selection Non-disclosure Agreement Used by the Air Force	47
Figure 5: Confidentiality Agreement Used by DOD's TRICARE Management Activity for Contractor Employees Providing Administrative Support into the Source-Selection Process	49
Figure 6: Non-disclosure Agreement for Contractor Employees and Subcontractors Used by DOD's TRICARE Management Activity	51
Figure 7: DHS Form 11000-6, Sensitive But Unclassified Information Non-disclosure Agreement DHS Requires from Contractors and Consultants	54
Figure 8: Non-disclosure Agreement Used by the Department of the Treasury for TARP Contractor Employees and Management Officials	58

Abbreviations

AFFARS	Air Force Federal Acquisition Regulation Supplement
BPA	blanket purchase agreement
CMS	Centers for Medicare & Medicaid Services
CUI	controlled unclassified information
DFARS	Defense Federal Acquisition Regulation Supplement
DHS	Department of Homeland Security
DOD	Department of Defense
FAR	Federal Acquisition Regulation
FISMA	Federal Information Security Management Act of 2002
FOIA	Freedom of Information Act
FOUO	for official use only
FPDS-NG	Federal Procurement Data System–Next Generation
HHS	Department of Health and Human Services
HHSAR	Department of Health and Human Services Acquisition Regulation
HIPAA	Health Insurance Portability and Accountability Act of 1996
HSAR	Department of Homeland Security Acquisition Regulation
HSPD-12	Homeland Security Presidential Directive 12
IT	information technology
OFPP	Office of Federal Procurement Policy
OMB	Office of Management and Budget
Privacy Act	The Privacy Act of 1974
SBU	sensitive but unclassified
TARP	Troubled Asset Relief Program
TMA	TRICARE Management Activity
Treasury	Department of the Treasury

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



United States Government Accountability Office
Washington, DC 20548

September 10, 2010

The Honorable Thomas R. Carper
Chairman
Subcommittee on Federal Financial Management, Government
Information, Federal Services, and International Security
Committee on Homeland Security and Governmental Affairs
United States Senate

Dear Mr. Chairman:

To a great extent, federal agencies rely on support contractor employees to help accomplish a broad array of complex and mission-critical functions.¹ In carrying out their day-to-day tasks for federal agencies in what the Office of Management and Budget (OMB) calls the multisector workforce,² contractor employees often require extensive access to and use of sensitive government information. Protection of sensitive information is critical because unauthorized disclosure can erode the integrity of government operations and lead to situations in which that information is misused for private gain, potentially harming important interests such as the privacy of individuals, commercial business proprietary rights, national security, and law enforcement. The risks associated with contractor misuse of sensitive information have been the subject of media attention, such as a recent case involving a contractor employee's theft of names, Social Security numbers, and dates of birth for Transportation Security Administration airport employees in Boston and a case involving State Department contractor employees' unauthorized viewing of the electronic passport files of three 2008 presidential candidates.

¹In fiscal year 2009 alone, federal agencies obligated \$332 billion for contracted services, such as support for acquisition management, program management, and quality assurance, which together accounted for approximately 61 percent of total fiscal year 2009 procurement dollars.

²Office of Management and Budget Memorandum, *Managing the Multi-Sector Workforce*, M-09-26 (July 29, 2009). As used in this report, "multisector workforce" includes the nongovernment contractor employees (and subcontractors to prime contractors) working in various agency offices with government employees. This can include situations in which the contractor personnel may be physically separated from government personnel at the agency worksite, but working in close proximity at adjacent locations to enable routine access to agency offices, officials, and information.

With the growth in use of contractors supporting government operations, the question of how best to limit contractor misuse and unauthorized disclosure of sensitive information becomes increasingly important. Many of the rules governing how contractors operate are articulated in the Federal Acquisition Regulations (FAR) system, which establishes uniform policies and procedures for acquisition of supplies and services by all executive agencies. It consists of the FAR and agency-specific regulations that supplement and implement the FAR with additional guidance to meet specific needs of the agencies.³ In its 2007 report, the Acquisition Advisory Panel reported a concern that not all federal agencies had established guidance for how support-services contractor employees should protect sensitive information such as confidential or proprietary data from release or improper use.⁴ The panel concluded that substantial benefits could be achieved if governmentwide guidance and contract clauses were developed in the FAR that federal agencies could use to protect sensitive information, rather than having agencies develop such clauses individually. Our work has reported similar concerns and is generally consistent with the panel's recommendations about the proper role of contractor employees in the multisector workforce.⁵

Given the government's reliance on contractors and their access to sensitive information, you asked us to review safeguards in the federal acquisition system to manage risks and control contractor access to sensitive information. Specifically, we assessed the (1) extent to which agency guidance and contracts contain safeguards for contractor access to sensitive information, and (2) adequacy of governmentwide guidance in the FAR on how agencies are to contractually safeguard sensitive information to which contractor employees may have access.

To assess agency guidance and contracts relating to contractor access to sensitive information, we analyzed the type of information agencies identify as requiring protection; limiting its disclosure; and prohibiting its

³FAR Subparts 1.1 and 1.3. The FAR and agency supplements are codified in title 48 of the Code of Federal Regulations.

⁴*Report of the Acquisition Advisory Panel to the Office of Federal Procurement Policy and the United States Congress* (January 2007). The Services Acquisition Reform Act of 2003, Pub. L. No. 108-136, § 1423 (2003) established an Acquisition Advisory Panel to make recommendations for improving acquisition practices.

⁵GAO, *Federal Acquisition: Oversight Plan Needed to Help Implement Acquisition Advisory Panel Recommendations*, [GAO-08-160](#) (Washington, D.C.: Dec. 20, 2007).

misuse based on (1) review of agency practices related to controls over contractor access to sensitive information, (2) review of applicable standards drawn from GAO's Standards for Internal Controls in the Federal Government,⁶ and (3) discussions with government security and contracting officials responsible for administrative, information, and contractor personnel security functions. To assess the extent to which agency guidance required the use of contract clauses and provisions to safeguard sensitive information, we selected three agencies that rank among the top procurers of contracted services in fiscal year 2008 and that our prior work shows rely extensively on contractors—the (1) Department of Defense (DOD), (2) Department of Homeland Security (DHS), and (3) Department of Health and Human Services (HHS). At all three agencies, we analyzed agency FAR supplements as well as policy and guidance regarding sensitive information safeguards. We also interviewed acquisition policy, security, and privacy officials to discuss their supplements to the FAR and the contract provisions they use to meet their specific agency needs. To assess the extent to which agency contracts contain such safeguards, we analyzed contract actions⁷ for services potentially requiring contractor access to sensitive information at DOD, DHS, and HHS. More specifically, at each of five organizational locations at DOD, DHS, and HHS, we analyzed documentation for a nongeneralizable sample of 6 to 10 (for a total of 42) contract actions for support services, selected because they involve contractors working in close proximity to government employees and to provide a cross section of services contracts to review by type and functions performed. The purpose of this contract analysis was to determine whether they contained contract provisions consistent with attributes we identified for safeguarding sensitive information from unauthorized contractor disclosure and misuse. We used content analysis to classify and code the information in the contract documents. Two GAO analysts independently reviewed the provisions and clauses in each contract or task order and

⁶[GAO/AIMD-00-21.3.1](#) (Washington, D.C.: November 1999). For example, the internal control standards call for restrictions on access to and accountability for resources and records, so that management assigns and maintains accountability.

⁷For purposes of this report, we define a contract action as a contract or task order, or both, and blanket purchase agreement (BPA) and its associated orders. The FAR defines a task order as an order for services placed against an established contract or with government sources. FAR Section 2.101. The FAR allows agencies to establish BPAs under the General Services Administration's schedules program, where contracts are awarded to multiple vendors for commercial goods and services and made available for agency use. FAR Subsection 8.405-3. BPAs are agreements between agencies and vendors with terms in place for future use; funds are obligated when orders are placed.

then reconciled any differences in how they were coded. For nine of the contract actions that we judgmentally selected for in-depth case studies, we also interviewed officials, such as contracting officers, program managers, contracting officers' representatives, and security and privacy officials.

To assess the adequacy of governmentwide guidance, we analyzed FAR requirements that prescribe protections associated with sensitive information. We also reviewed proposed and pending amendments to the FAR. To further understand steps being taken to amend the FAR, we interviewed officials at the Office of Federal Procurement Policy (OFPP) in OMB and other agencies with FAR Council membership.⁸ We conducted this performance audit from May 2009 through September 2010 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. Additional details of our objectives, scope, and methodology are included in appendix I.

Background

Unauthorized disclosure of sensitive information by government or contractor employees through negligence or misconduct can have a significant effect on the government's ability to perform its primary functions, potentially resulting in financial loss, damaged reputation, and loss of public trust. Sensitive information may not always be explicitly designated or marked as such. For the purposes of this report, we use the term "sensitive information" to generally refer to information under an agency's authority or control that has a degree of confidentiality⁹ such that

⁸The FAR Council—whose members include the DOD Director of Defense Procurement and Acquisition Policy, the National Aeronautics and Space Administration Associate Administrator for Procurement, and the General Services Administration Chief Acquisition Officer—oversees development and maintenance of the FAR. The Administrator of OFPP in OMB serves as chair of the FAR Council, which meets quarterly to discuss and resolve significant or controversial FAR changes. Proposed and final revisions to the FAR are published in the Federal Register.

⁹For the purposes of this report, we use the definition of confidentiality provided in the Federal Information Security Management Act of 2002, Pub. L. No. 107-296, § 1001 (44 U.S.C. § 3532). The act states that confidentiality means preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

its loss, misuse, unauthorized access, or modification could compromise that confidentiality and harm important interests, such as personal and medical privacy to which individuals are entitled under laws,¹⁰ national security, law enforcement, proprietary commercial rights, or the conduct of agency programs.

The large but unquantifiable amount of sensitive information generated by the government makes understanding its scope more difficult and agencies' safeguarding this information from unauthorized disclosure or inappropriate use by contractors a complex challenge. Table 1 shows examples of several types of sensitive information. Additional examples are listed in appendix II. All examples were drawn from a myriad of designations that agencies use to describe sensitive information.

¹⁰The Privacy Act of 1974 (Privacy Act), Pub. L. No. 93-579 (codified at 5 U.S.C. § 552a) regulates the federal government's use of personal information by placing limitations on agencies' collection, disclosure, and use of personal information in systems of records. The Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191 (HIPAA) among other things, addresses the personal and medical privacy of individuals. Issued under HIPAA, the federal Privacy Rule provided individuals with new protections regarding the confidentiality of their health information and established new responsibilities for health care providers, health plans, and other entities, including the federal government, to protect such information.

Table 1: Examples of Sensitive Information

Type of information	Description	Examples
Personal	The terms personal information and personally identifiable information can be used interchangeably to refer to any Privacy Act–protected information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity; (2) any other information that is linked or linkable to an individual.	<ul style="list-style-type: none"> • Name • Social Security number • Date and place of birth • Mother's maiden name • Biometric records • Patient health and medical information • Educational information • Financial information • Employment information • Census data • Taxpayer data
Source selection	Nonpublic information prepared for use by an agency to evaluate a bid or proposal to enter into an agency procurement contract, such as contractor's proposed costs or the government's evaluation plans.	<ul style="list-style-type: none"> • Contractor bid or proposal information, including cost or pricing data • Source-selection plans • Technical evaluation plans • Technical evaluations of proposals • Cost or price evaluations of proposals • Rankings of bids, proposals, or competitors • Competitive range determinations • Evaluations of source-selection panels, boards, or advisory councils
Business proprietary	Nonpublic information that is used, produced, or marketed under legal rights of the business concern.	<ul style="list-style-type: none"> • Information that may relate to trade secrets, processes, operations, style of work, or apparatus • Information that may relate to the identity, confidential statistical data, amount or source of any income, profits, losses, or expenditures • Information about manufacturing processes, operations, or techniques marked proprietary by a business concern
Agency sensitive	Information relating to an agency's mission, management operations, or staff that is generally not released to the public. Each agency may individually determine what qualifies as this type of information, therefore, the type of information covered by this category varies by agency.	<ul style="list-style-type: none"> • Continuity-of-operations information • Security management information • System and network monitoring information • Predecisional planning, programming, budgeting, and execution documents and information • Protection services (building security) • Personnel records

Source: GAO analysis of laws, regulations, and other government sources.

The federal government uses a variety of means, whether prescribed by statute, executive order, or other authority, to limit dissemination and

protect against the inadvertent disclosure of certain types of sensitive information. For information the government considers critical to our national security, the government may take steps to protect such information by classifying it as Top Secret, Secret, or Confidential pursuant to criteria established by law and executive order.¹¹ Information that does not meet the thresholds established for classification as national security information but that an agency nonetheless considers sufficiently sensitive to warrant restricted dissemination has generally been referred to as sensitive but unclassified (SBU). In designating information this way, agencies determine that the information they use must therefore be safeguarded from public release. Some, but not all, SBU designations used by agencies have a specific basis in statute.

For example, some agencies use the provisions of the Freedom of Information Act (FOIA)¹² as their basis for designating information as SBU. FOIA establishes that federal agencies must generally provide the public with access to government information, thus enabling them to learn about government operations and decisions. FOIA establishes a legal right of access to government records and information, on the basis of the principles of openness and accountability in government. But the act also prescribes nine specific categories of information that are exempt from disclosure: for example, trade secrets and certain privileged commercial or financial information, certain personnel and medical files, and certain law enforcement records or information.¹³ Thus the need to safeguard sensitive information from public disclosure while striking the appropriate balance with the goal of government transparency is another challenge agencies must continually address. Protecting legitimate security, law enforcement, and privacy interests also must be carefully balanced with protecting civil liberties. Of critical importance are providing clear rules to those who handle sensitive information and ensuring that the handling and

¹¹See Executive Order 13526, *Classified National Security Information* (Dec. 29, 2009). Among other provisions, the executive order prescribes the categories of information that warrant classification and prescribes standards for safeguarding classified materials.

¹²5 U.S.C. § 552. See GAO, *Freedom of Information Act: Requirements and Implementation Continue to Evolve*, [GAO-10-537T](#) (Washington, D.C.: Mar. 18, 2010).

¹³See [GAO-10-537T](#), which provides the complete list of the nine categories of information that are exempt from disclosure under FOIA, in attachment 1. In denying access to material, agencies may cite these exemptions. The act requires agencies to notify requesters of the reasons for any adverse determination (that is, a determination not to provide records) and grants requesters the right to appeal agency decisions to deny access.

dissemination of information is not restricted unless there is compelling need.

Government ethics rules prohibit federal employees from using sensitive nonpublic information, defined below, for personal gain or to further the interests of another, whether by advice or recommendation or through knowing unauthorized disclosure. For federal employees, certain activities and acts that affect a personal financial interest may also result in violations of criminal law with potentially serious consequences, including dismissal, prosecution, fines, and imprisonment.¹⁴ Because not all government ethics rules and related statutes apply to contractors, many of these prohibitions do not extend to contractor employees working in the multisector workforce.

Nonpublic Information as Defined in Government Ethics Rules

Nonpublic information is information that the employee gains by reason of federal employment and that s/he knows or reasonably should know has not been made available to the general public. It includes information that s/he knows or reasonably should know:

1. Is routinely exempt from disclosure under the Freedom of Information Act, codified at 5 U.S.C. § 552, or otherwise protected from disclosure by statute, Executive order or regulation;
2. Is designated as confidential by an agency; or
3. Has not actually been disseminated to the general public and is not authorized to be made available to the public on request.

Source: GAO analysis of 5 C.F.R. 2635.703 (b).

Safeguards to Protect Sensitive Information Not Always Available in Agency Guidance or Included in Contract Actions

Our analysis of guidance and contract actions at three agencies found areas where sensitive information is not fully safeguarded and thus may remain at risk of unauthorized disclosure or misuse. DHS, DOD, and HHS FAR supplements include some guidance and standard contract provisions—for example that address contractor safeguards for personal information. However, the policies and procedures available in DOD's and HHS's FAR guidance do not contain effective agency management controls for sensitive information needed to help ensure contractor compliance, prevent contractor disclosure and misuse, and promote contractor accountability. Such guidance could help contracting and program officials incorporate safeguards into their contract actions for protecting

¹⁴ 18 U.S.C. § 1905 (disclosure of confidential information generally) and 18 U.S.C. § 208 (acts affecting a personal financial interest).

all types of relevant sensitive information contractors may access, such as agency sensitive information. At the contract level, almost half of the 42 contract actions reviewed did not include solicitation and contract provisions that safeguarded against unauthorized contractor disclosure and inappropriate use of sensitive information contractors may access in program offices during the course of contract performance.¹⁵ In cases where there was agency policy to include contract provisions to protect sensitive information on all contracts, such as regarding the medical privacy of individuals, it was not incorporated in 5 of the 42 contract actions that we reviewed. Additionally, DOD and HHS lack guidance on the use of nondisclosure agreements, while DHS has found that these help improve accountability by informing contractors of their responsibilities and the consequences that may result from their failure to meet those responsibilities.

Attributes of Safeguards Needed in Agency Guidance and Contracts to Protect Sensitive Information

Contractor and subcontractor employees can be responsible for carrying out a range of mission-critical tasks—including studying ways to acquire desired capabilities, developing contract requirements, and advising or assisting on source selection, budget planning, financial management, and regulations development—potentially requiring access to many types of sensitive information. Agencies can use their FAR supplement authority to issue guidance, which may include contract provisions to establish contractor responsibility for safeguarding sensitive information.¹⁶

Review of agency practices and discussions with government security and contracting officials identified three key attributes for assessing the extent that agencies' guidance or the FAR contain effective safeguards for sensitive information in acquisition guidance and contracts. On the basis of these sources, in order to have more effective safeguards in place, contracts should contain provisions that (1) describe the relevant scope of sensitive information under the agency's authority or control that should

¹⁵Our review included contracts, task orders, and BPAs and their associated orders. We reviewed one BPA that did not include provisions that fully safeguarded against unauthorized contractor disclosure and inappropriate use of sensitive information; however, we did not review any orders off this agreement, and these may have contained additional clauses to protect sensitive data.

¹⁶Agencies are authorized to issue regulations that implement or supplement the FAR and incorporate agency policies, procedures, contract clauses, solicitation provisions, and forms that govern the contracting process or otherwise control the relationship between the agency and contractors or prospective contractors. FAR Subpart 1.3.

be protected if contractors require access to it for contract purposes; (2) require the contractor to refrain from disclosing such sensitive information to anyone except as needed for contract performance; and (3) address conflicts of interest or other misuse by prohibiting the contractor from using such sensitive information for any purpose other than contract performance.

Agency FAR guidance should help contracting and program officials incorporate effective safeguards for sensitive information into their contract actions by including certain management control practices. We identified a range of management control practices sometimes incorporated into acquisition guidance to help prevent contractor disclosure and misuse, and promote contractor accountability for sensitive information breaches that harm important interests. These control practices include requiring contractors to (1) train or inform employees on their obligations to maintain confidentiality and not misuse sensitive information; (2) obtain written consent from the agency to disclose sensitive information; (3) pass sensitive information provisions to subcontractors; (4) execute a nondisclosure agreement for each employee and subcontractor as a condition of access to sensitive information; (5) promptly notify key agency officials of the misuse or unauthorized disclosure of sensitive information; and (6) be informed of the consequences for violations.

Agency Guidance for Two of Three Agencies Reviewed Lacks Needed Safeguards for Contractor Protection of Sensitive Information

Our review found DOD, DHS, and HHS all have guidance that supplements the FAR and addresses requirements or standard contract provisions for contractor protection of certain categories of sensitive information. For example, DOD supplements the protection of individual privacy requirements contained in the FAR by incorporating references to the agency rules and regulations.¹⁷ HHS also supplements the FAR with detailed policy that establishes Privacy Act requirements and requires the inclusion of contract provisions to protect the confidentiality of records and the privacy of individuals in contracts where the Privacy Act is not applicable but the contract would involve the collection of individually identifiable personal information by the contractors.¹⁸

¹⁷Defense Federal Acquisition Regulation Supplement (DFARS) Subpart 224.1, Protection of Individual Privacy.

¹⁸Department of Health and Human Services Acquisition Regulation (HHSAR), Subpart 324.1, Protection of Individual Privacy.

However, with respect to other key attributes available in agency FAR policies and procedures reviewed at DOD, DHS, and HHS, the agencies' guidance differs in how well they help contracting and program officials incorporate necessary safeguards for sensitive information into their contract actions. Of the guidance analyzed at the three agencies, only DHS established effective management control practices through standard contract provisions in its FAR supplement and related guidance requiring contractors to safeguard sensitive information accessed by employees. In contrast, the FAR guidance of DOD and HHS does not contain effective agency management controls for sensitive information needed to help ensure contractor compliance, prevent contractor disclosure and misuse, and promote contractor accountability. (See app. III for the standard contract provisions we identified in DHS, DOD, and HHS FAR supplements.)

As shown in table 2, our analysis of agency guidance included in the DHS FAR supplement found that it contained five of six effective management control practices consistent with key attributes for establishing safeguards for sensitive information. For example, the DHS FAR supplement and related guidance aims to (1) make contractors aware of their responsibilities for maintaining confidentiality of sensitive information; (2) address conflicts of interest and potential misuse by prohibiting use of agency information processed, stored, or transmitted by the contractor for any purpose other than contract performance; and (3) deter noncompliance with these requirements and ensure accountability by explaining consequences related to violations. According to agency acquisition policy officials, recognition within DHS of the need for contractor safeguards for homeland security-sensitive information likely led to the establishment of extensive requirements when the agency updated its interim FAR supplement and related guidance in 2006. On the other hand, DHS acquisition policy and security officials acknowledge that the agency's FAR supplement and contract clause do not directly specify contractor responsibilities for promptly notifying contracting officers of

unauthorized use or disclosure of sensitive information.¹⁹ Prompt contractor notification to key government officials is critical to avoid internal delays that would prevent officials from being aware of the unauthorized use or disclosure; delay agency decisions about how to respond; and deny the opportunity for affected parties to take precautions.

¹⁹Under incident reporting procedures contained in a DHS security management directive, with which the Department of Homeland Security Acquisition Regulation (HSAR) states compliance is required in all contracts that require access to sensitive information, DHS employees or employees of contractors who observe or become aware of the loss, compromise, suspected compromise, or unauthorized disclosure of “for official use only” (FOUO) information (a type of sensitive information) are required to report it immediately, but not later than the next duty day, to the originator and the local security official. Other than this requirement, the DHS directive does not establish other contractor responsibilities, such as prompt notification to the contracting officer.

Table 2: Analysis of Control Practices in Agency FAR Supplements for Safeguarding Sensitive Information Accessed by Contractors

Applicable FAR supplement guidance	Requires contractor employee training on protection and disclosure of sensitive information	Requires written consent to disclose	Requires prompt notification to agency of unauthorized disclosure or misuse	Requires employees sign nondisclosure agreements	Requires passing of safeguards to subcontractors	Explains that there are consequences for violations
DHS HSAR Section 3004.470—Security requirements for access to unclassified facilities, Information Technology resources and sensitive information ^a	✓	✓		✓	✓	✓
DOD DFARS Subsection 204.404-70—directs contracting officers to use the clause, Disclosure of Information ^b , when the contractor will have access to or generate unclassified information that may be sensitive and inappropriate to release to the public		✓			✓	
HHS HHSAR Subpart 324.70—Confidentiality of Information (deleted) ^c		✓				

Source: GAO analysis of DOD, DHS, and HHS data.

Notes: Data are from agency FAR supplements. See app. III for the full text of the DHS, DOD, and HHS contract clauses cited in this analysis.

^aThe Department of Homeland Security Acquisition Regulation (HSAR) directs contracting officers to include the basic clause, HSAR Subsection 3052.204-71, Contractor Employee Access, when contractor employees require recurring access to government facilities or access to sensitive information. Subsection 3004.470-2 requires compliance with the policies and procedures in a DHS security management directive that expressly requires contractor and consultants to execute the DHS Form 11000-6, Sensitive But Unclassified Information Non-disclosure Agreement, as a condition of access to sensitive information. See appendix IV for detailed information about DHS contractor nondisclosure agreement requirements.

^bDefense Federal Acquisition Regulation Supplement (DFARS) Subsection 252.204-7000. Our analysis on this chart is limited to the noted DFARS clause and corresponding subsection. Other DFARS clauses may contain some of these safeguards to protect sensitive information, but they are limited to specific categories of information. For example, as a condition of access to another contractor's technical data or computer software delivered to the government, DFARS 227.7103-7 provides that an authorized company representative may execute a nondisclosure agreement directly with the other contractor that prohibits (1) use of such data for other than government contract purposes and (2) release, display, or disclosure of such technical data or computer software without the express written permission of the other contractor. Under this DFARS provision, execution of this nondisclosure agreement is for the benefit of the other contractor, and the recipient contractor agrees to hold harmless the government from every liability arising out of the misuse of the other contractor's technical data or computer software.

^cContracting officers were directed to use the clause in Department of Health and Human Services Acquisition Regulation (HHSAR) Subsection 352.224-70, Confidentiality of Information, whenever the need existed to keep information confidential, such as when contracts involved the use of proprietary plans or processes or confidential financial information of organizations other than the contractor's. When HHS revised its FAR supplement effective as of January 2010, this guidance was removed in its entirety from the HHSAR.

DHS's guidance establishes stronger safeguards for sensitive information than what we found at DOD and HHS in their FAR supplements. In contrast with the DHS guidance, the analysis in table 2 shows that DOD's FAR supplement does not include the same amount of detail as to how contractors are to safeguard sensitive information. At present, DOD's FAR supplement is limited to requiring the use of a disclosure of information clause in solicitations and contracts when contractors have access to unclassified information that may be sensitive and inappropriate for release to the public—for example, DOD officials said the clause authorizes use in a contractor's press and marketing materials.²⁰ In addition, since HHS revised its FAR supplement as of January 2010,²¹ guidance and a contract provision that required contractors to obtain written consent before disclosing certain kinds of sensitive information—not already subject to FAR and agency privacy restrictions—was deleted

²⁰DFARS 204.4, Safeguarding Classified Information Within Industry. In March 2010, an advance notice of proposed rulemaking was published in the Federal Register. These proposed changes would add a new subpart and associated contract clauses to DFARS for the safeguarding, proper handling, and cyber intrusion reporting of unclassified DOD information resident or transiting on contractor IT systems. 75 Fed. Reg. 9563 (Mar. 3, 2010). The proposed changes do not address safeguards for contractor employee access to sensitive information in DOD's IT systems. A revised draft proposed rule is planned for September 2010.

²¹HHS revised its FAR supplement effective January 2010 to reflect statutory, FAR, and governmentwide and HHS policy changes since the last revision in December 2006. Final Rule, Health and Human Services Acquisition Regulation (HHSAR), 74 Fed. Reg. 62396-472 (Nov. 27, 2009).

in its entirety.²² According to the director for acquisition policy, HHS deleted the “Confidentiality of Information” clause because the need for agency guidance will be obviated by pending changes to the FAR expected later in 2010.²³

Besides the supplemental FAR guidance, agencies have developed other policies and control practices to establish additional contractor responsibilities for safeguarding certain categories of sensitive information obtained during contract performance. For example, a 2007 privacy breach involving a DOD contractor that potentially compromised the personal health information of 580,000 households led the privacy office in DOD’s component agency TRICARE Management Activity (TMA) to determine that the agency’s contract provisions did not adequately protect sensitive information.²⁴ According to the TMA privacy office director, most TMA contracts before 2007 did not specifically require the contractor to safeguard personal health information, notify DOD or beneficiaries of privacy breaches, or to mitigate any harm, such as paying for the cost of free credit monitoring to affected individuals.

To address this problem, TMA has required since 2007 that standard contract provisions be included whenever a contract is awarded that requires either the use of or access to personal information. The required contract language is posted on TMA’s Web site and imposes protections for the privacy and security of personally identifiable information and protected health information. It seeks to ensure that contractors understand their responsibility in protecting TRICARE beneficiaries’ sensitive information. Similarly, HHS’s Centers for Medicare and Medicaid Services (CMS) issued an acquisition policy and procedure notice, which took effect in 2005, to advise contracting staff of the requirement to use a

²² HHSAR 324.70—Confidentiality of Information (Dec. 20, 2006). This clause related to confidential information, which was defined as (1) information or data of a personal nature about an individual or (2) proprietary information or data submitted by or pertaining to an institution or organization.

²³ The pending changes referred to by the official are included in FAR Case No. 2007-019, Contractor Access to Non-Public Information.

²⁴ According to DOD’s privacy incident report, the information that was breached was from a single contractor-owned server in Florida used to hold and transfer data between individuals in different locations to perform contract services. Potentially compromised files included sensitive personal information such as name, social security number, address, date of birth, medical record number, insurance information, and information related to medical appointments and delivery of health care services.

clause for contractor protection of health information. This standard CMS clause had been revised to integrate the HIPAA security standards along with the privacy standards that were previously adopted in standard contract provisions.²⁵

Almost Half of Contract Actions Reviewed Lack Contract Provisions That Fully Safeguard Sensitive Information

For our analysis of contract documents for 42 contract actions at DHS, DOD, and HHS that involved contractor employees supporting mission-critical tasks, in order to be considered to fully safeguard all types of sensitive information, a contract had to contain provisions that specifically required contractors to refrain from (1) disclosing sensitive information to anyone except as needed for contract performance and (2) using such sensitive information for any purpose other than contract performance. In addition, the provisions had to cover the relevant types of sensitive information that may be accessed by a contractor during performance. As shown in table 3, our analysis found that slightly more than half of contract actions reviewed—23 of 42—contained contract provisions that fully safeguard the confidentiality and appropriate use of all types of sensitive information. In contrast, the remaining 19 contract actions reviewed did not extend safeguards to all relevant types of sensitive information that contractors may have had access to through the program offices they support. In the absence of such safeguards, there is higher risk of unauthorized disclosure or misuse of sensitive information by contractors.²⁶

²⁵Centers for Medicare and Medicaid Services (CMS), Acquisition Policy & Procedure Notice 12, Privacy Rule HIPAA Business Associate Contract Provision II (Baltimore, Md.: Apr. 21, 2005).

²⁶We did not consider the absence of such contract provisions as a deficiency unless they were also required by agency policy or the FAR.

Table 3: Analysis of Contract Provisions Establishing Contractor Safeguards for Sensitive Information

Agency	Number of contracts reviewed	Presence of provisions safeguarding sensitive information ^a	Absence of provisions safeguarding sensitive information
DHS	14	11	3
DOD	18	9	9
HHS	10	3	7
Total	42	23	19

Source: GAO analysis of agency contracts.

^aAnalysis of 23 contract actions found evidence of contract provisions that established requirements for appropriate disclosure, handling, access, and restrictions on misuse of a full range of nonpublic agency information, proprietary information, and privacy information.

Of the 19 contracts reviewed that did not have provisions for all safeguards, our content analysis found that one HHS blanket purchase agreement and an associated order we reviewed contained no evidence of contract provisions for contractor safeguarding of sensitive information, except for standard FAR clauses related to the Privacy Act in the base contract. In addition, some contract provisions included in 18 other contract actions provided too few safeguards, given the range of tasks being performed and the potential opportunities to gain access to many types of sensitive information. For example, at HHS several contract actions specified that contractors must safeguard certain types of sensitive information, but did not specify contractor protection of agency-sensitive information from nondisclosure or misuse. In other cases, clauses addressed limitations on the disclosure of certain types of sensitive information, but not its misuse, and therefore did not fully safeguard these types of information. Some HHS contract actions require that contractors perform acquisition functions related to other contractors, such as strategic planning in support of future task awards or auditing business proposals, and thus could require access to proprietary information. These contract actions did not always include safeguards addressing limits on unauthorized disclosure and misuse of proprietary information. Similarly, several DOD contract actions included provisions to prevent contractors from disclosing any nonpublic information they obtained during contract performance, but provisions to prohibit contractors from misusing the information for purposes other than contract performance were absent.

In cases where there was agency policy to include specific contract provisions to protect sensitive information, it was not incorporated in five of the contract actions we reviewed. For example, 3 DHS task orders of

the 14 contract actions reviewed did not include the contract clause required when contractors need recurring access to government facilities or sensitive information.²⁷ At HHS, 2 task orders of the 10 contract actions reviewed did not include standard contract provisions regarding HIPAA privacy and security standards required by agency policy to be in all contracts.

Two of Three Agencies Reviewed Lack Guidance on Using Contractor Nondisclosure Agreements for Full Range of Sensitive Information

Several of the contract actions we reviewed used nondisclosure agreements as a mechanism to help protect sensitive information from conflicts of interest and preserve its confidentiality. These agreements generally outline the exchange of confidential information or knowledge that at least two parties need to share for certain purposes, but wish to restrict access to by third parties. When used by agencies as a condition of contractor access to sensitive information, a nondisclosure agreement may serve several important accountability purposes. These include informing contractor employees and subcontractors of (1) the trust that is placed in them by providing them access to sensitive information; (2) their responsibilities to protect that information from unauthorized disclosure and use; and (3) the consequences that may result from their failure to meet those responsibilities.

All of the agencies we reviewed had established guidance requiring contractor employees participating in source-selection activities to sign an agreement to not disclose procurement sensitive, proprietary, or source-selection information. Beyond addressing this one area of sensitive information however, only DHS and TMA (in DOD) had guidance requiring the use of standard contractor nondisclosure agreements for a broader range of sensitive information that may be handled by contractors. Under the DHS and TMA guidance, certain contracts are to contain provisions that require contractors to submit to a designated agency official an executed nondisclosure agreement for each employee and subcontractor within a stipulated time following contract award or before they are given access to certain types of agency sensitive information. Appendix IV provides examples of standard nondisclosure agreements we reviewed.

DHS and TMA security and acquisition policy officials responsible for jointly developing agency guidance on nondisclosure agreements view these agreements as critical to promoting contractor accountability.

²⁷HSAR 3052.204-71.

According to the DHS administrative security chief, the agencywide nondisclosure agreement was developed in coordination with agency acquisition policy, information technology (IT) security, and privacy officials to educate contractor personnel on the agency's standards for safeguarding sensitive information and provide a mechanism to hold them accountable should they violate the terms of the agreement. The agencywide form was also developed to eliminate use of nonstandard forms to cover different types of sensitive information that were causing confusion and required contractor employees to sign multiple forms.²⁸ According to DOD's acquisition executive for TMA, having contractor employees sign nondisclosure agreements provides additional benefits for the government by (1) requiring that contractors will protect and not disclose sensitive information; (2) protecting against conflicts of interest that could occur if contractors use sensitive information for future competitive advantage; and (3) making contractors and their employees aware of the government's expectations and their obligations to safeguard sensitive information.

As shown in table 4, due to the agencywide use of nondisclosure agreements at DHS and DOD's TMA, 20 of 42 contract actions reviewed contained contract provisions requiring nondisclosure agreements for each employee and subcontractor. All 10 of the Air Force contracts reviewed and 1 contract at HHS required contractors to enter into third-party agreements with other contractors about the confidentiality and use of their proprietary information obtained during contract performance.

²⁸In May 2010, DHS notified the heads of its contracting activities to caution their acquisition personnel to use only the official agency nondisclosure agreement, DHS Form 11000-6, from the agency's internal forms Web site. DHS took this action after we alerted them that case study contracts we had reviewed were using an unauthorized variation of the form that was missing date blocks for both the agreement signatory and witness. According to DHS, any agreement that lacks signature dates is incomplete and provides inadequate protection to the signatories since there is no record of when the agreement takes effect. The May 2010 updates to agency guidance and electronic contract writing system require contracting personnel to use the forms Web site to access DHS Form 11000-6.

Table 4: Analysis of Contract Requirements for Nondisclosure Agreements

Agency	Number of contract actions reviewed	Contract provisions relating to nondisclosure agreements		
		Requires contractor to submit executed nondisclosure agreement for each individual as a condition of access	Requires contractor agreements with third-parties to protect their proprietary information	Does not require nondisclosure agreements
DHS	14	12	0	2 ^a
DOD				
TMA	8	8	0	0
Air Force	10	0	10	0
HHS	10	0	1	9
Total	42	20	11	11

Source: GAO analysis of agency contracts and task orders.

^aDHS policy requires nondisclosure agreements to be executed by contractors as a condition of access to sensitive information. Therefore, these contractors may have been required to sign nondisclosure agreements, but this requirement was not clearly stated in two contracts.

One case study of an Air Force contract illustrated the practical challenges for agency monitoring of such third-party agreements in contrast to agency use of its own contractor nondisclosure agreements. In this case study, although the contractor’s conflict of interest mitigation plan indicated the company maintained nondisclosure agreements and proprietary protection agreements with many third-party contractors, no copies of executed nondisclosure agreements were available from the Air Force contracting and program officials responsible for administering the contract. In addition, officials told us they knew that the contractor had entered into such agreements, but they had not reviewed them.²⁹

We discussed a less challenging approach for implementing agency contractor nondisclosure agreements with the Department of the Treasury’s (Treasury) contract administrator responsible for management and oversight of contractors and financial agents supporting the Troubled Asset Relief Program (TARP).³⁰ He agrees with DHS and TMA views that

²⁹ Air Force informational guidance on the use of such third-party “associate contractor agreements” suggests standard contract provisions requiring the contractor to provide the contracting officer a copy of the document for review before execution by the cooperating contractors.

³⁰ We have reported extensively on Treasury’s management and oversight of contractors and financial agents to support TARP. For more information, see GAO, *Troubled Asset Relief Program: One Year Later, Actions Are Needed to Address Remaining Transparency and Accountability Challenges*, [GAO-10-16](#) (Washington, D.C.: Oct. 8, 2009).

nondisclosure agreements are critical to promoting contractor accountability for maintaining confidentiality of sensitive information and providing other benefits, such as helping to prevent conflicts of interest that could arise from contractor misuse of the information. Treasury uses an alternative way to implement these agreements that reduces administrative burden without compromising contractor compliance for their use. Language included in certain TARP Financial Agency Agreements requires the financial agent to have each employee and all affiliate and contractor personnel to whom nonpublic information is or may be disclosed execute the agency's nondisclosure agreement form— included as an exhibit to the agreement—as a condition of access to sensitive government information.³¹ According to the Treasury official, it is better to have the contractor responsible for retaining the executed agreements in its own files, rather than have the government contracting officer or program office retain them. The official explained that as long as the terms of the contract require contractors to certify to the government they have collected the agency's nondisclosure agreement for all individuals they assign to perform on the contract, and the agreements are available to the government for inspection, it is better to hold contractors accountable for retaining the signed agreements.

Efforts Underway to Improve Governmentwide Guidance in the FAR for Contractor Access to Sensitive Information

The FAR Council in recent years has made progress improving guidance for security and oversight related to contractor access to sensitive government facilities and information systems, but challenges remain. While the FAR establishes governmentwide guidance on certain contractor sensitive-information safeguards prescribed in statute—for example, to require contractor protection of individual privacy—FAR guidance does not address certain key areas relating to contractor access to sensitive information. Several amendments are pending before the FAR Council to implement recommended changes and to improve FAR guidance in the complex areas involving contractor access to sensitive information. Such changes to the FAR could provide agencies clear guidance on the use of contractor nondisclosure agreements as a condition of access to sensitive information and could include requirements for contractors to promptly notify agencies of unauthorized disclosure and misuse of sensitive information to enable timely decisions regarding an agency's response when use of sensitive information is

³¹ An example of Treasury's nondisclosure agreement used for TARP support contractors is included in appendix IV.

compromised. With the rulemaking process underway to develop these amendments, the FAR Council has an opportunity to consider additional changes to strengthen FAR guidance to ensure remaining gaps in contractor safeguards identified in this review are addressed.

**Governmentwide
Guidance Currently
Addresses Certain
Contractor Safeguards for
Sensitive Information**

The FAR is the primary regulation that provides uniform policies and procedures for acquisitions by executive agencies.³² During the acquisition process, the FAR emphasizes basic planning that has to be coordinated among agency personnel responsible for significant aspects of the acquisition, such as contracting, fiscal, legal, and technical personnel.³³ In describing agency needs during acquisition planning, the FAR directs agencies to address all significant considerations that will control each acquisition, including security considerations for acquisitions requiring routine contractor physical access to a federal facility or IT system.

The FAR has several provisions that establish policy and contract clauses implementing requirements prescribed in statute or executive order for contractor protection of certain categories of sensitive information, such as information related to the privacy of individuals. When these FAR provisions, which are described in table 5, are applicable, certain sensitive-information requirements are included in solicitation and contract provisions that are intended to safeguard procurement integrity, classified information, organizational conflicts of interest, and privacy.³⁴ Agencies use this guidance to incorporate requirements during acquisition planning and when describing agency needs.

³²The FAR contains the rules, standards, and requirements for the award, administration, and termination of government contracts.

³³FAR Subpart 7.1.

³⁴An organizational conflict of interest may result when factors create an actual or potential conflict of interest on an instant contract, or when the nature of the work to be performed on the contract creates an actual or potential conflict of interest on a future acquisition. For example, these conflicts may arise in situations in which a current or prospective contractor or subcontractor will have access to, or had access to, nonpublic information that may provide an unfair competitive advantage in a future acquisition.

Table 5: FAR Contract Provisions for Safeguarding Certain Types of Sensitive Information

Covered information	FAR provisions obliging contractor employee authorized use and confidentiality
Source selection	Section 3.104—Procurement Integrity. Both federal employees and contractor employees that have access to contractor bid or proposal information or source-selection information are subject to laws and regulations to limit disclosure of protected procurement-related information. Violations are punishable by both civil and criminal penalties and administrative actions, such as contract cancellation. 41 U.S.C. § 423.
Classified	Subpart 4.4—Safeguarding Classified Information Within Industry. Contracting officers shall review all proposed solicitations to determine whether access to classified information may be required by offerors or by a contractor during contract performance. If so, the contracting officer shall follow the relevant agency's procedures for security clearances. Contracting officers shall also include the appropriate security requirements clause (52.204-2) in solicitations and contracts for security safeguards. During the award phase of a "classified" contract, contracting officers for agencies covered by the national industrial security program shall use the Contract Security Classification Specification (DD Form 254) to inform contractors and subcontractors of the security classifications and requirements assigned to the various documents, materials, tasks, and subcontracts.
Business proprietary	Subsection 9.505-4—Obtaining Access to Proprietary Information. FAR subpart 9.5 requires contracting officers to identify and evaluate potential organizational conflicts of interest prior to contract award and take steps to address potential conflicts that they determine to be significant. The contracting officer may use solicitation provisions or a contract clause to require agreements about restrictions on the use of other contractors' proprietary information obtained during the course of contract performance to prevent the contractor from gaining an unfair advantage. These restrictions encourage companies to provide information necessary for contract performance. If the contracting officer imposes the restrictions, the contractor that gains access to proprietary information of other contractors must agree with other companies to protect their information from unauthorized use or disclosure and refrain from using the information for any purpose other than necessary for contract performance. If such agreements are required, the contracting officer shall obtain copies of these agreements and ensure that they are properly executed.
Personal	Subpart 24.1—Protection of Individual Privacy. In implementing federal privacy requirements the FAR requires that when an agency contract will involve the design, development, or operation of a system of records on individuals to accomplish an agency function, the contracting officer shall (1) ensure that the contract identifies the system of records on individuals and the design, development, or operation work to be performed, and (2) make available agency rules and regulations implementing the Privacy Act. A contractor and its employees may be subject to criminal penalties for violation of the Privacy Act. 5 U.S.C. § 552a.

Source: GAO analysis of the FAR.

Finally, to address the need for improved governmentwide contracting guidance required by presidential directive or law and to assist agencies in addressing identified risks from contractor access to sensitive federal facilities and information systems, OFPP and the FAR Council revised contractor personnel and IT security requirements in the FAR. Key aspects of the revised contractor personnel and IT security safeguards are summarized as follows:

- Securing personal identity verification of contractor personnel—in 2007 the FAR was amended in part to implement the August 2004 Homeland Security Presidential Directive 12 (HSPD-12), which required the

establishment of a governmentwide standard for secure and reliable forms of identification for federal employees and contractors alike.³⁵

Implementing HSPD-12 requirements through contract provisions may help address the risks of contractors gaining unauthorized physical or electronic access to federal information or contractors using outmoded identification cards that can be easily forged, stolen, or altered to allow unauthorized access.

- Strengthening federal information security oversight of contractor IT operations—in 2005 an interim rule amended the FAR to implement the Federal Information Security Management Act of 2002 (FISMA) information-technology-security provisions.³⁶ According to the FAR Council, the addition of specific FISMA-related provisions was intended to provide clear, consistent guidance to acquisition officials and program managers, and to encourage and strengthen communication with IT security officials, chief information officers, and other affected parties.

See appendix V for greater detail on these changes to the FAR.

Addition of Recommended Changes in FAR Contract Provisions Underway to Improve Sensitive Information Safeguards

There have been numerous recommendations in recent years for improved governmentwide guidance and contract provisions for contractor protection of sensitive information. The emphasis has been on standardizing approaches and establishing accountability mechanisms when access to information is compromised. Problems and recommendations to address them include the following:

- In 2007, the Acquisition Advisory Panel found that increased use of contractor employees in the government workforce to support the evaluation of other contractors raises questions regarding the potential for organizational conflicts of interest and how to preserve the confidentiality of proprietary information. To address such risks, the panel recommended that the FAR Council provide additional regulatory guidance for contractor access to and responsibilities for protecting proprietary information belonging to other companies. It specifically called for developing standardized contract provisions and approaches for agencies' use of nondisclosure agreements and in creating remedies for improper

³⁵Final Rule, FAR Case 2005-017, *Requirement to Purchase Approved Authentication Products and Services*, amended FAR Subpart 4.13 and 52.204-9. 72 Fed. Reg. 46333-35 (Aug. 17, 2007).

³⁶Interim Rule, FAR Case 2004-018, *Information Technology Security*, 70 Fed. Reg. 57449-52, (Sept. 30, 2005). A year later, after consideration of public comments, the interim rule was adopted without change.

information sharing. It also suggested the use of standardized clauses for organizational conflicts of interest to address issues of unfair competitive advantage when a firm gains access to information as part of its performance of government contract responsibilities.

- Similarly, on the basis of lessons learned from agency responses to loss of personally identifiable information, in April 2007 we noted that agencies need to clearly define contractor responsibilities for protecting privacy information.³⁷ In this report, contractors were prominently involved in privacy data breaches at three of six agencies reviewed, including one case in which a contractor inadvertently released informational compact discs to several FOIA requesters that contained Social Security numbers and tax identification data on 350,000 individuals receiving government program payments. We noted that contractor obligations for mitigating damage from data breaches, such as notifying affected individuals or providing credit monitoring, may be unclear unless specified in the contract. Consistent with and in response to our report, DHS acquisition policy officials told us in June 2009 of their recommendations for revisions to the FAR Subpart 24.1 to (1) expand existing Privacy Act coverage and (2) implement a standard approach that promotes contractor accountability. According to DHS officials, to avoid agency-by-agency development of inconsistent clauses or other contractual terms, the FAR needs a revised privacy policy and clause for establishing basic government and contractor and subcontractor expectations, roles, and responsibilities—including prompt breach notification procedures for contractors to inform officials of privacy data breaches to enable the agency’s timely response.
- Additionally, in 2008 we reported that certain defense contractor employees who support key mission-critical tasks that have the potential to significantly influence DOD decisions are not subject to the same ethical safeguards as federal employees.³⁸ Furthermore, no FAR policy obliges government agencies using these contractor employees to require that they be free from personal conflicts of interest or addresses the issue

³⁷GAO, *Privacy: Lessons Learned about Data Breach Notification*, [GAO-07-657](#) (Washington, D.C.: Apr. 30, 2007). The loss of personally identifiable information, such as an individual’s Social Security number, name, and date of birth can result in serious harm, including identity theft. Identity theft occurs when such information is used without authorization to commit fraud or other crimes.

³⁸GAO, *Defense Contracting: Additional Personal Conflict of Interest Safeguards Needed for Certain DOD Contractor Employees*, [GAO-08-169](#) (Washington, D.C.: Mar. 7, 2008). A proposed FAR rule would define “personal conflict of interest” as a situation in which a contractor employee has a financial interest, personal activity, or relationship that could impair the employee’s ability to act impartially and in the best interest of the government when performing under the contract.

of contractor employee misuse of the government's nonpublic information obtained while performing work under a contract for private gain. To address this problem, we recommended that DOD develop and implement policy that would require a contract clause, among other safeguards, to prohibit contractor personnel from using nonpublic government information for personal gain. DOD postponed implementing the recommendation once OFPP and the FAR Council began responding to legislation from Congress.³⁹ Among other changes, the legislation required a standard policy to be developed and issued to prevent personal conflicts of interest by contractor employees performing acquisition functions closely associated with inherently governmental functions. This policy was to require each contractor whose employees performed these functions to prohibit covered employees with access to nonpublic government information from using it for personal gain.

In response, since 2007 the FAR Council has opened several cases, shown in table 6, to amend the FAR to provide additional regulatory coverage and clauses. These open cases, with implementing regulations pending as of July 2010, have significant potential for addressing these identified problems. Discussions with OFPP and DOD officials responsible for these FAR changes, and review of information they provided on these cases, indicate that the steps the FAR Council has been taking to revise governmentwide guidance are consistent with the recommendations. For example, a review of information on these pending FAR cases indicates significant changes are being considered to amend the FAR so that it addresses access to nonpublic information and conflicts of interest. Changes being considered also contain other policies and clauses consistent with safeguards we identified for protecting contractor sensitive information, and these changes may mitigate the risks of unauthorized disclosure and misuse. FAR cases generally follow a lengthy process that allows the public, as well as federal agencies, to comment on proposed changes to the FAR. Because of other rulemaking priorities and the many steps involved—including legal and interagency reviews—FAR Council officials told us the rulemaking process could take many more months to complete.

³⁹Duncan Hunter National Defense Authorization Act for Fiscal Year 2009, Pub. L. No. 110-417, § 841 (2008). In addition, section 841 requires that the Administrator of OFPP develop FAR policies and clauses effective no later than August 10, 2009, for inclusion in solicitations, contracts, task orders, and delivery orders to prevent personal conflicts of interest by contractor employees performing acquisition functions closely associated with inherently governmental functions.

Table 6: Status of Pending FAR Cases to Revise Policies and Clauses for Contractor Use and Confidentiality of Sensitive Information

FAR case	Synopsis	Significance	Status as of July 2010
2007-019, Contractor Access to Non-public Information	Consideration of how to safeguard nonpublic information by including provisions and clauses in solicitations and contracts for the use of nondisclosure agreements; information sharing among contractors; and remedies for improper disclosure.	Could potentially address gaps in the FAR's regulatory coverage responsive to Acquisition Advisory Panel's recommended improvements	FAR case opened in 2007; proposed rule has yet to be published in Federal Register for consideration of public comment. FAR staff is awaiting additional government input on draft proposed rule after review by defense and civilian agency acquisition councils.
2007-018, Organizational Conflicts of Interest	Consideration of whether current guidance on organizational conflicts of interest is adequate for assisting current needs of agencies or whether providing standard provisions or clauses might be helpful.	Could potentially address Acquisition Advisory Panel recommendations by changing current guidance under FAR 9.505-4 that allows agencies to impose restrictions on contractors gaining access to proprietary information from others in the performance of a government contract to avoid unfair advantage and protect their information from unauthorized use or disclosure.	FAR case opened in 2007; proposed rule has yet to be published in Federal Register for consideration of public comment. Draft proposed rule is under review by OFPP.
2008-025, Preventing Personal Conflicts of Interest by Contractor Employees Performing Acquisition Functions	Implements § 841(a) of the Duncan Hunter National Defense Authorization Act for Fiscal Year 2009, Pub. L. No. 110-417, that required OFPP to develop and issue a policy and clauses for inclusion in solicitations, contracts, task orders, and delivery orders. Proposes a definition of "non-public government information," adapted from government ethics rules, as meaning any information that a covered employee gains by reason of work under a contract and that the covered employee knows, or reasonably should know, has not been made public (e.g., proprietary contractor information in the possession of the government).	Also may address GAO recommendation for DOD to develop a policy that will prohibit contractors performing acquisition functions with access to nonpublic government information obtained while performing work under the contract from using it for personal gain. Use of the proposed clause would require contractors to obtain nondisclosure agreements from covered employees and report to the contracting officer any personal conflict of interest violation. Also lists remedies available to the government if a contractor fails to comply with the requirements, such as payment suspension or contract termination.	FAR case opened in 2008; proposed rule published in Federal Register for consideration of public comment in November 2009. ⁸ Public comments have been addressed by FAR staff for draft final FAR rule; awaiting interagency concurrence on open issues before final rule can be published in Federal Register.

FAR case	Synopsis	Significance	Status as of July 2010
2009-022, Security of Systems Handling Sensitive Personally Identifiable Information	Would establish a uniform approach for handling of sensitive Privacy Act information.	Could potentially address GAO recommendation and DHS-proposed revision.	FAR case opened in 2009; proposed rule yet to be published in Federal Register for consideration of public comment. Draft proposed rule is under OMB review

Source: GAO analysis of FAR Council information.

^aThe FAR Council issued the proposed rule, Federal Acquisition Regulation: FAR Case 2008-025, Preventing Personal Conflicts of Interest for Contractor Employees Performing Acquisition Functions. Public comments were due in January 2010. 74 Fed. Reg. 58584-89 (Nov. 13, 2009).

Opportunity Exists for FAR Council to Consider Additional Changes in the FAR to Further Address Safeguards for Contractor Access to Sensitive Information

Until the FAR Council completes the rulemaking process for the pending cases listed in table 6, it is unclear the extent to which the changes will address risks and better control contractor confidentiality and authorized use of sensitive information. With regard to unauthorized disclosure and use of sensitive information, these risks include (1) unauthorized access by contractor employees or subcontractors not involved with contract performance, (2) conflicts of interest in using sensitive information for financial gain or unfair competitive advantage, and (3) unauthorized disclosure.

Similarly to issues we identified in agency guidance, our review found that FAR guidance does not address certain areas relating to contractor access to sensitive information. Moreover, rather than having agencies develop stronger safeguards individually, the FAR Council is developing a standardized approach to address many of these areas. This is particularly relevant with regard to changes being considered under the open FAR Case 2007-019, Contractor Access to Non-Public Information, listed above. Nevertheless, our review of potential changes to FAR guidance identified two key areas yet to be addressed where the FAR does not contain guidance that could help agencies address problems identified in this report.

The first key area is the development and use of contractor nondisclosure agreements as a condition of access to sensitive information. Additional FAR guidance also could ensure nondisclosure agreements used across the government include clear and complete information to contractors. Without uniform emphasis in the FAR on how agencies use contractor nondisclosure agreements, contractors may not be adequately informed of their responsibilities to protect that information from unauthorized

disclosure and use and the consequences that may result from their failure to meet those responsibilities.

The second key area is the establishment of requirements for contractors to provide agencies prompt notification of deviations by their employees or subcontractors from provisions for use and confidentiality of all types of sensitive information.⁴⁰ Without such guidance in the FAR, contractors may not be adequately required to make key government officials aware of unauthorized disclosure or inappropriate use of sensitive information involving their employees. A contractor's prompt notification is critical to avoiding delays in internal agency decisions about how to respond to the misuse or unauthorized disclosure of sensitive information and the opportunity for affected parties to take precautions. Also, without such guidance, agencies may be less able to act on a timely basis to hold contractors accountable for their failure to properly use and maintain confidentiality of sensitive information.

Conclusions

The government's extensive use of contractors in the multisector workforce to support management activities and administrative functions, coupled with contractors' increasing access to government facilities, has in recent years prompted several constructive efforts by the FAR Council to establish uniform contract provisions. However, of the three agencies reviewed for this report, only DHS has established guidance for controlling contractor use and limiting unauthorized disclosure of sensitive information obtained during contract performance. OFPP and the FAR Council have recognized that FAR guidance does not address certain key areas. Rather than having agencies develop their own guidance and clauses individually, several amendments are pending to improve guidance and contract clauses in the FAR. While these are steps in the right direction, opportunities exist to address certain gaps we identified in pending FAR guidance. These include the need for guidance on agency use of contractor nondisclosure agreements and the need to establish requirements for contractors to promptly notify agencies of unauthorized disclosure or misuse of sensitive information, which is critical to enabling timely agency decisions and responses.

⁴⁰Pending FAR cases may result in requirements for prompt notification of unauthorized disclosure or misuse, but will not necessarily apply to all types of sensitive information.

Recommendations for Executive Action

To address the need for clearly defining contractor responsibilities in governmentwide guidance in the FAR, we recommend that the Administrator of OFPP ensures that the FAR Council incorporates changes in the FAR that address safeguards for contractor access to sensitive information by

- providing guidance to agency acquisition policy officials, in coordination with IT security and privacy officials, chief information officers, and other affected parties, on agency development and use of contractor nondisclosure agreements as a condition of access to sensitive information; and
- establishing a requirement for prompt notification to appropriate agency officials of a contractor's unauthorized disclosure or misuse of sensitive information so that timely agency responses are facilitated and appropriate contractor accountability mechanisms can be enforced.

Agency Comments and Our Evaluation

We provided a draft of this report to OMB's OFPP, DOD, HHS, and DHS for review and comment. In oral comments, OFPP generally concurred with our recommendations. DOD provided technical comments that were incorporated into the report as appropriate and HHS did not have comments.

In written comments, included in appendix VI, DHS generally concurred with our report. However, DHS took exception to the analysis for 1 of the 14 contract actions reviewed, which we found did not contain adequate safeguards to protect sensitive information. While we agree that the task order identified in DHS' response includes contract provisions with prohibitions against disclosing sensitive information, the language does not address safeguards to ensure contractors' appropriate use of sensitive information.

DHS also stated that although this task order lacks a contract clause required in DHS acquisition regulations, it includes comparable provisions in the statement of work. We reviewed the task order and the guidance for the clause HSAR 3052.204-71, Contractor Employee Access, which requires the use of the clause or one substantially the same in solicitations and contracts when contractor employees require recurring access to government facilities or access to sensitive information. On the basis of our review, we continue to believe that the task order does not contain HSAR clause 3052.204-71 or a contract clause that is substantially the same as that clause. Although some provisions in the task order contain similar information and requirements, these provisions do not cover the same breadth or detail as HSAR clause 3052.204-71. For example, the task order

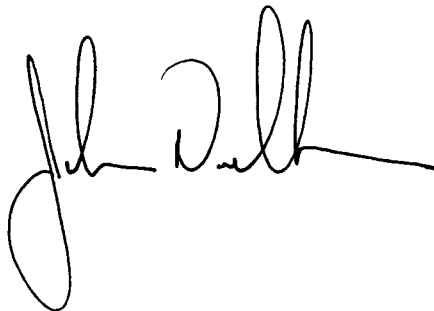
does not include a comprehensive definition section such as the one in HSAR clause 3052.204-71. Without the use of such comprehensive definitions, it is not clear that the various provisions of the task order noted by DHS collectively and effectively protect the same range of sensitive government information as set forth in HSAR clause 3052.204-71. In addition, the task order specified in DHS' response does not include provisions that limit contractors from disclosing sensitive information without authorization from the contracting officer. Also, the portions of the statement of work cited as comparable with HSAR clause 3052.204-71(e) relate specifically to information technology, and not necessarily to information that contractors and their employees may otherwise gain access to in the course of their contractual responsibilities.

DHS also provided technical comments, which were incorporated into the draft where appropriate.

We are sending copies of this report to the Director of OMB; the Secretaries of Defense, Homeland Security, and Health and Human Services; and interested congressional committees. The report also is available at no charge on GAO's Web site at <http://www.gao.gov>.

If you or your staff have any questions concerning this report, please contact me at (202) 512-4841 or needhamjk1@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made major contributions to this report are listed in appendix VII.

Sincerely yours,

A handwritten signature in black ink, appearing to read 'John K. Needham', with a stylized, cursive script.

John K. Needham
Director, Acquisition and Sourcing Management

Appendix I: Scope and Methodology

To assess the extent that agency guidance and contracts establish effective safeguards for sensitive information, we identified key attributes of the safeguards that should be contained in acquisition guidance and contracts to manage the risks of contractor unauthorized disclosure and misuse based on (1) review of agency practices related to controls over contractor access to sensitive information, (2) review of applicable standards drawn from GAO's Standards for Internal Control in the Federal Government,¹ and (3) discussions with government security and contracting officials responsible for administrative, information, and contractor personnel security functions. Specifically the acquisition guidance and contracts should contain safeguards that (1) describe the relevant scope of sensitive information under the agency's authority or control that should be protected if contractors require access to it for contract purposes, (2) require the contractor to refrain from disclosing such sensitive information to anyone except as needed for contract performance, and (3) prohibit the contractor from using such sensitive information for any purpose other than contract performance.

To assess the extent to which agency guidance contains safeguards for contractor protection of sensitive information, we analyzed applicable guidance available in the respective Federal Acquisition Regulation (FAR) supplements of the Department of Defense (DOD), the Department of Homeland Security (DHS), and the Department of Health and Human Services (HHS). We selected these departments for review because they ranked among the top procurers of contracted services in fiscal year 2008, based on a review of the Federal Procurement Data System-Next Generation (FPDS-NG), and because prior GAO work shows that their component agencies and organizations rely extensively on support contractors to perform mission-critical tasks that would potentially require access to sensitive information. We assessed the reliability of the FPDS-NG data through corroboration with agency officials and contract files and determined they were sufficiently reliable for our purposes. We analyzed applicable policy and guidance available from the departments and some of their selected component agencies and organizations to identify the extent their guidance provides for contractor protection of sensitive information, including guidance contained in agency FAR supplements as well as security and privacy program policies and procedures applicable to contractor employees. We also interviewed acquisition policy, security,

¹[GAO/AIMD-00-21.3.1](#) (Washington, D.C.: November 1999).

and privacy officials to discuss their supplements to FAR guidance and the contract provisions they use to meet their specific agency needs.

To assess the extent to which agency contracts contain safeguards for contractor protection of sensitive information, we analyzed DOD, DHS, and HHS contract actions (defined as a contract, task order, and blanket purchase agreement and associated order) for services potentially requiring contractor access to sensitive information from the following five component agencies or organizations and locations:

- within DOD, the (1) TRICARE Management Activity (TMA) in Falls Church, Virginia, and the contracting activity supporting TMA at the U.S. Army Medical Research Acquisition Activity at Fort Detrick, Maryland, and (2) the Air Force Materiel Command's Electronic Systems Center at Hanscom Air Force Base, Massachusetts;
- within DHS in Washington, D.C., (3) U.S. Customs and Border Protection and (4) the Office of Procurement Operations within the Office of the Chief Procurement Officer, which is the contracting activity supporting headquarters organizations; and
- within HHS, the (5) Centers for Medicaid and Medicare Services (CMS) in Baltimore, Maryland.

At each of these five organizations, we selected for review a nongeneralizable sample of 6 to 10 contract actions (42 in total) in which contractor employees worked in close proximity to government employees and provided professional and administrative services that supported the agencies' missions, in addition to providing a cross section of contract types and services. In making our selection, we reviewed lists of contract actions and reported dollar values drawn from data provided by DOD, DHS, and HHS component agency and organization officials to confirm that the contract actions belonged to their agencies and that they involved contractors working on-site or in close proximity with government employees, to perform services potentially requiring access to sensitive information.

For each of the 42 contract actions, we analyzed the contract documentation provided, including base contracts from which task orders or blanket purchase agreements and their associated orders were issued, to determine whether they contained provisions or clauses that direct contractors to safeguard sensitive information consistent with key attributes we identified for safeguarding sensitive information. In conducting this content analysis, two GAO analysts independently reviewed the provisions in each contract or task order and then reconciled any differences in how they were coded. We determined whether the

contract provisions addressed limiting disclosure of sensitive information and preventing its misuse. We also assessed the scope of information protected—whether these protections applied to certain categories or to all relevant types of sensitive information that may potentially have been accessed during contract performance. We also determined whether the contract actions required the use of contractor nondisclosure agreements.

To obtain an in-depth understanding of the reasons why certain contract clauses and provisions to safeguard sensitive information were required and obtain views on their effectiveness and how contractor compliance with the requirements was being monitored by the government at a cross section of DOD, DHS, and HHS offices, we selected 9 of the 42 contract actions as case studies. For each case study, we conducted semistructured interviews with the DOD, DHS, or HHS officials responsible for developing contract requirements and monitoring contractor performance, including contracting officers, contracting officers' representatives, and program managers.

To assess the adequacy of governmentwide guidance in the FAR on how agencies are to contractually safeguard sensitive information to which contractor employees have access, we analyzed FAR requirements that prescribe protections associated with sensitive information, including Part 4 (Administrative Matters); Part 7 (Acquisition Planning); Subpart 9.5 (Organizational and Consultant Conflicts of Interest); Part 24 (Protection of Privacy and Freedom of Information); and Part 52 (Solicitation Provisions and Contract Clauses). We reviewed pending amendments to the FAR and legislation to determine the safeguards they might add to existing FAR guidance. To further understand steps being taken to amend the FAR, we interviewed government officials supporting members of the FAR Council, which oversees the development and maintenance of the FAR, and officials with the Office of Federal Procurement Policy (OFPP) in the Office of Management and Budget. The OFPP Administrator serves as chair of the FAR Council.

We conducted this performance audit from May 2009 through September 2010 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: Sensitive But Unclassified Markings Identified by President’s Task Force on Controlled Unclassified Information

In 2006 we reported on a survey of federal agencies that showed 26 were using 56 different designations to protect information they deem critical to their missions—such as law-enforcement sensitive, sensitive security information, and unclassified controlled nuclear information.¹ Because of the many different and sometimes confusing and contradictory ways that agencies identify and protect sensitive but unclassified (SBU) information, the sharing of information about possible threats to homeland security has been difficult.²

To address this challenge, efforts are underway to establish new governmentwide processes for designating, marking, safeguarding, and disseminating SBU information. Since 2008, in response to a presidential memorandum that replaced SBU information with “controlled unclassified information” (CUI) as the single categorical designation for SBU information, the executive branch is attempting to overhaul its CUI framework.³ The ongoing effort is also addressing a 2009 presidential task force report that found too many labels for sensitive information and recommended that agencies reduce them and balance the need for nondisclosure (to protect privacy or other legitimate interests) and transparency and openness in government.⁴

The task force found that currently, across the executive branch, this information is identified by over 100 unique markings and at least 130 different labeling or handling regimes (a partial listing of SBU markings

¹GAO, *Information Sharing: The Federal Government Needs to Establish Policies and Processes for Sharing Terrorism-Related and Sensitive but Unclassified Information*, [GAO-06-385](#) (Washington, D.C.: Mar. 17, 2006).

²Since 2005, the issue of establishing effective mechanisms for sharing terrorism-related information to protect the homeland has been on GAO’s high-risk list of federal functions needing broad-based transformation. Since then, we have monitored the government’s progress in resolving barriers to sharing. See GAO, *Information Sharing: Definition of the Results to Be Achieved in Terrorism-Related Information Sharing Is Needed to Guide Implementation and Assess Progress*, [GAO-08-637T](#) (Washington, D.C.: July 23, 2008).

³See Presidential Memorandum, *Memorandum for the Heads of Executive Departments and Agencies: Designation and Sharing Controlled Unclassified Information* (May 9, 2008).

⁴Report and Recommendations of the Presidential Task Force on Controlled Unclassified Information (Aug. 25, 2009). The president’s memorandum of May 27, 2009, on Classified Information and Controlled Unclassified Information directed the task force, led by the Secretary of Homeland Security and the Attorney General, to review the controlled unclassified information framework established in 2008 for the management of sensitive but unclassified terrorism-related information.

**Appendix II: Sensitive But Unclassified
Markings Identified by President's Task Force
on Controlled Unclassified Information**

the task force found currently in use are shown below). The SBU challenge, according to the task force, is that although SBU regimes or markings are typically derived from an identifiable authority, collectively they reflect a disjointed, inconsistent, and unpredictable system for protecting, sharing, and disclosing sensitive information.

Table 7: Selected SBU Markings Currently in Use

Acquisition Sensitive	Agency Internal Use Only (U//AIUO)	Attorney Client	Attorney/Client Privileged
Attorney Work Product	Bank Secrecy Act Information (BSA)	Budgetary Information	CALEA Cost Recovery Information (CALEA)
CFIUS Information (CFIUS)	Chemical-Terrorism Vulnerability Information (CVI)	Child Victim/Witness (CH)	Close Hold
Commercial Markings	Communication/Attorney Work Product (PRV)	Computer Security Act Sensitive Information (CSASI)	Confidential Business Information (CBI)
Confidential Contract Proposal Information (CCPI)	Confidential Information Protection and Statistical Efficiency Act of 2002 (CIPSEA)	Contractor Access Restricted Information (CARI)	Contractual Sensitive Information
Controlled Nuclear Information (U//DCNI or U//ECNI)	Copyright (Date) (Owner)	Covered by Confidentiality Agreement	DEA Sensitive (DEA S)
Deliberate Process Privilege	Dissemination Is Prohibited Except As Authorized by AR 20-1	Do Not Disseminate	DOD Unclassified Controlled Nuclear Information (DOD UCNI)
Enforcement Confidential Information (ECI)	Exclusive Distribution (EXDIS or XD)	Export Controlled Information (Or Material) (ECI)	Eyes Only
Federal Taxpayer Information	Financial Records (NON-NSL) (FR)	Financial Records NSL (NSLF)	For Internal Use Only
For Official Use Only (FOUO)	For Official Use Only-Law Enforcement Sensitive (FOUO-LES)	Foreign Intelligence Surveillance Act (FISA)	Grand Jury Material (FGJ)
Government Purpose Rights	Health Related Information (EM)	Innocent Images Visual Information (IIVI)	Innovation Research Information and Small Business
IT Security Related	Juvenile-Protect Identity in Accordance With 18 USC 5031 (JI)	LAN Backup Sensitive Information	LAN Infrastructure
Law Enforcement Sensitive (LES)	Limited Access	Limited Credit Information NSL (NSLC)	Limited Distribution (LIMDIS)
Limited Official Use (LOU)	Limited Official Use Information (LOUI)	Limited Official Use-Law Enforcement Sensitive (LOU-LES)	Limited Rights
Limited Use Only (LUO)	Medical Records	Naval Nuclear Propulsion Information (NOFORN)	Naval Nuclear Propulsion Information (U-NNPI)
No Distribution (NODIS or ND)	Not For Distribution Safeguards Information (SGI)	Official Use Only (OUO)	Official Use Only-Applied Technology

**Appendix II: Sensitive But Unclassified
Markings Identified by President's Task Force
on Controlled Unclassified Information**

Official Use Only-Export Controlled Information	Official Use Only-Patent Caution Information	Official Use Only-Protected Cooperative Census Confidential	Official Use Only-Sensitive Internal Information
Official Use Only-Small Business	Operations Security Protected Information (OSPI)	Originator Controlled (ORCON)	Personally Identifiable Information- Privacy Act of 1974
Personnel Data, Privacy Act of 1974 (5 U.S.C. 552A)	Predecisional Product	Pre-decisional	Pre-Existing Markings
Privacy Act Protected Information (PAPI)	Privileged FBI Attorney Client	Proprietary Information (PROPIN)	Protected Critical Infrastructure Information (PCII)
RELIDO	Research and Development Agreement Information	Restricted Access	Restricted By Court Order (CO)
Restricted Rights	RSEN	SBU-GSA-BI	SBU-NF
SBU/NOFORN	Select Agent Sensitive Information (SASI)	Sensitive (SENS)	Sensitive But Unclassified (SBU)
Sensitive Drinking Water Related Information (SDWRI)	Sensitive Homeland Security Information (SHSI)	Sensitive Information (SINFO)	Sensitive Information-Special Handling Required
Sensitive Security Information (SSI)	Sensitive Student Records (STR)	Sensitive Treaty/MOU/NDA Information (STM)	Sensitive Unclassified Non- Safeguards Information (SUNSI)
Sensitive Water Vulnerability Assessment Information	Small Business Innovation Research (SBIR) Program	Special License Rights	Source Selection Information
Source Selection Sensitive	Substance Abuse Records (SAB)	Technology Transfer Information	Telephone or Electronic Communications NSL (NSLT)
Title III Communications (T3)	Trade Secret	Trade Sensitive Information	Unlimited Rights

Source: Presidential Task Force on Controlled Unclassified Information

Note: Data are from the Report and Recommendations of the Presidential Task Force on Controlled Unclassified Information (Aug. 25, 2009).

Appendix III: Agency Contract Provisions Containing Contractor Safeguards for Sensitive Information

Our analysis of agency Federal Acquisition Regulation (FAR) supplements for the Department of Homeland Security (DHS), the Department of Defense (DOD), and the Department of Health and Human Services (HHS) identified the following examples of contract clauses and provisions that establish safeguards for contractor access to sensitive information.

DHS

The Department of Homeland Security Acquisition Regulation (HSAR) Subpart 3004.4, Safeguarding Classified and Sensitive Information Within Industry (48 C.F.R. 3004), states that contracting officers shall insert the clause at HSAR 3052.204-71, shown in figure 1, or one substantially the same, in solicitations and contracts when contractor employees require recurring access to government facilities or access to sensitive information. The clause shall not be used unless contractor employees will require recurring access to government facilities or access to sensitive information.

Figure 1: HSAR Clause 3052.204-71, Contractor Employee Access

3052.204-71 Contractor employee access.

As prescribed in (HSAR) 48 CFR 3004.470-3(b), insert a clause substantially the same as follows with appropriate alternates:

**CONTRACTOR EMPLOYEE ACCESS
(JUN 2006)**

(a) *Sensitive Information*, as used in this Chapter, means any information, the loss, misuse, disclosure, or unauthorized access to or modification of which could adversely affect the national or homeland security interest, or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:

(1) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Public Law 107-296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, Part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);

(2) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, "Policies and Procedures of Safeguarding and Control of SSI," as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee);

(3) Information designated as "For Official Use Only," which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a

**Appendix III: Agency Contract Provisions
Containing Contractor Safeguards for
Sensitive Information**

(Continued)

person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and

(4) Any information that is designated "sensitive" or subject to other controls, safeguards or protections in accordance with subsequently adopted homeland security information handling procedures.

(b) "Information Technology Resources" include, but are not limited to, computer equipment, networking equipment, telecommunications equipment, cabling, network drives, computer drives, network software, computer software, software programs, intranet sites, and internet sites.

(c) Contractor employees working on this contract must complete such forms as may be necessary for security or other reasons, including the conduct of background investigations to determine suitability. Completed forms shall be submitted as directed by the Contracting Officer. Upon the Contracting Officer's request, the Contractor's employees shall be fingerprinted, or subject to other investigations as required. All contractor employees requiring recurring access to Government facilities or access to sensitive information or IT resources are required to have a favorably adjudicated background investigation prior to commencing work on this contract unless this requirement is waived under Departmental procedures.

(d) The Contracting Officer may require the contractor to prohibit individuals from working on the contract if the government deems their initial or continued employment contrary to the public interest for any reason, including, but not limited to, carelessness, insubordination, incompetence, or security concerns.

(e) Work under this contract may involve access to sensitive information. Therefore, the Contractor shall not disclose, orally or in writing, any sensitive information to any person unless authorized in writing by the Contracting Officer. For those contractor employees authorized access to sensitive information, the contractor shall ensure that these persons receive training concerning the protection and disclosure of sensitive information both during and after contract performance.

(f) The Contractor shall include the substance of this clause in all subcontracts at any tier where the subcontractor may have access to Government facilities, sensitive information, or resources.

(End of clause)

**ALTERNATE I
(JUN 2006)**

When the contract will require contractor employees to have access to Information Technology (IT) resources, add the following paragraphs:

(g) Before receiving access to IT resources under this contract the individual must

(Continued)

receive a security briefing, which the Contracting Officer's Technical Representative (COTR) will arrange, and complete any nondisclosure agreement furnished by DHS.

(h) The contractor shall have access only to those areas of DHS information technology resources explicitly stated in this contract or approved by the COTR in writing as necessary for performance of the work under this contract. Any attempts by contractor personnel to gain access to any information technology resources not expressly authorized by the statement of work, other terms and conditions in this contract, or as approved in writing by the COTR, is strictly prohibited. In the event of violation of this provision, DHS will take appropriate actions with regard to the contract and the individual(s) involved.

(i) Contractor access to DHS networks from a remote location is a temporary privilege for mutual convenience while the contractor performs business for the DHS Component. It is not a right, a guarantee of access, a condition of the contract, or Government Furnished Equipment (GFE).

(j) Contractor access will be terminated for unauthorized use. The contractor agrees to hold and save DHS harmless from any unauthorized use and agrees not to request additional time or money under the contract for any delays resulting from unauthorized use or access.

(k) Non-U.S. citizens shall not be authorized to access or assist in the development, operation, management or maintenance of Department IT systems under the contract, unless a waiver has been granted by the Head of the Component or designee, with the concurrence of both the Department's Chief Security Officer (CSO) and the Chief Information Officer (CIO) or their designees. Within DHS Headquarters, the waiver may be granted only with the approval of both the CSO and the CIO or their designees. In order for a waiver to be granted:

(1) The individual must be a legal permanent resident of the U. S. or a citizen of Ireland, Israel, the Republic of the Philippines, or any nation on the Allied Nations List maintained by the Department of State;

(2) There must be a compelling reason for using this individual as opposed to a U. S. citizen; and

(3) The waiver must be in the best interest of the Government.

(l) Contractors shall identify in their proposals the names and citizenship of all non-U.S. citizens proposed to work under the contract. Any additions or deletions of non-U.S. citizens after contract award shall also be reported to the contracting officer.

(End of clause)

(Continued)

**ALTERNATE II
(JUN 2006)**

When the Department has determined contract employee access to sensitive information or Government facilities must be limited to U.S. citizens and lawful permanent residents, but the contract will not require access to IT resources, add the following paragraphs:

(g) Each individual employed under the contract shall be a citizen of the United States of America, or an alien who has been lawfully admitted for permanent residence as evidenced by a Permanent Resident Card (USCIS I-551). Any exceptions must be approved by the Department's Chief Security Officer or designee.

(h) Contractors shall identify in their proposals, the names and citizenship of all non-U.S. citizens proposed to work under the contract. Any additions or deletions of non-U.S. citizens after contract award shall also be reported to the contracting officer.

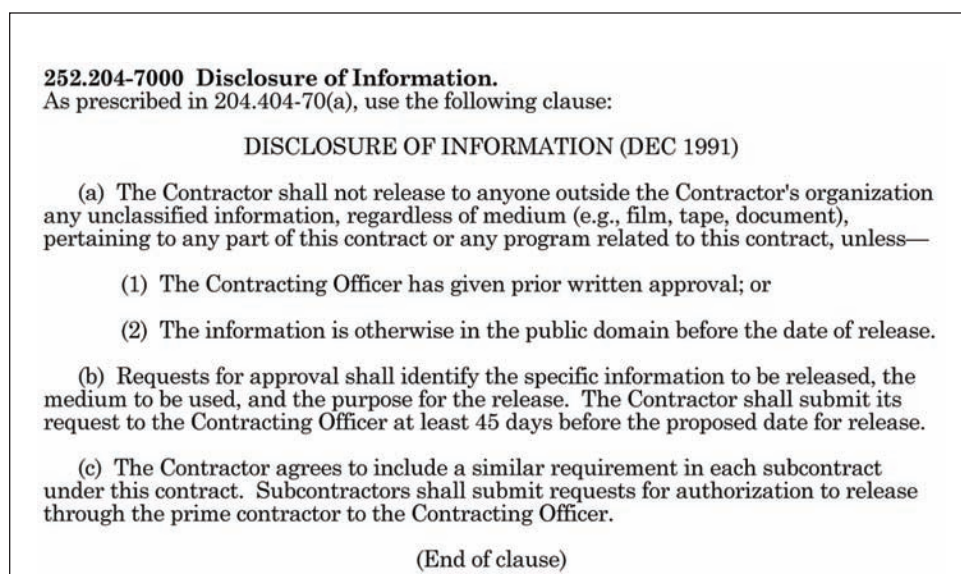
(End of clause)

Source: DHS.

DOD

The Defense Federal Acquisition Regulation Supplement (DFARS) Subpart 204.4, Safeguarding Classified Information Within Industry (48 C.F.R. 204.4), states DFARS clause 252.204-7000, Disclosure of Information (shown in fig. 2), should be used in solicitations and contracts when the contractor will have access to or generate unclassified information that may be sensitive and inappropriate to release to the public.

Figure 2: DFARS Clause 252.204-7000, Disclosure of Information



Source: DOD.

HHS

Guidance and contract provisions available in the Department of Health and Human Services Acquisition Regulation (HHSAR) Subpart 324.70, Confidentiality of Information (48 C.F.R. 324.70) (2006), and the accompanying contract clause, shown in figure 3, were deleted when HHS revised the HHSAR, effective January 2010.¹ The previous subpart stated that it was HHS policy to protect the personal interest of individuals, corporate interests of nongovernment organizations, and the capacity of the government to provide public services when information about those interests is obtained by contractors in performance of HHS contracts. The subpart further stated that this protection depended on the contractor's recognition and proper handling of the information.

The "Confidentiality of Information" contract clause shown in figure 3 was to be used in solicitations and resultant contracts whenever the need existed to keep information confidential, for example in contracts that

¹HHS, Final Rule, Health and Human Services Acquisition Regulation, 74 Fed. Reg. 62396-472 (Nov. 26, 2009).

involve the use of proprietary plans or processes or confidential financial information of organizations other than the contractors. In addition, any solicitation or contract including this clause was to indicate, as specifically as possible, the types of data that would be covered and the requirements for handling the data.

Figure 3: HHSAR 352.224-70, Confidentiality of Information

352.224-70 Confidentiality of information.

The following clause covers the policy set forth in subpart 324.70 and is used in accordance with the instructions set forth in 324.7004.

CONFIDENTIALITY OF INFORMATION (JAN 2006)

(a) Confidential information, as used in this clause, means information or data of a personal nature about an individual, or proprietary information or data submitted by or pertaining to an institution or organization.

(b) The Contracting Officer and the Contractor may, by mutual consent, identify elsewhere in this contract specific information and/or categories of information which the Government will furnish to the Contractor or that the Contractor is expected to generate which is confidential. Similarly, the Contracting Officer and the Contractor may, by mutual consent, identify such confidential information from time to time during the performance of the contract. Failure to agree will be settled pursuant to the "Disputes" clause.

(c) If it is established elsewhere in this contract that information to be utilized under this contract, or a portion thereof, is subject to the Privacy Act, the Contractor

**Appendix III: Agency Contract Provisions
Containing Contractor Safeguards for
Sensitive Information**

(Continued)

will follow the rules and procedures of disclosure set forth in the Privacy Act of 1974, 5 U.S.C. 552a, and implementing regulations and policies, with respect to systems of records determined to be subject to the Privacy Act.

(d) Confidential information, as defined in paragraph (a) of this clause, shall not be disclosed without the prior written consent of the individual, institution, or organization.

(e) Whenever the Contractor is uncertain with regard to the proper handling of material under the contract, or if the material in question is subject to the Privacy Act or is confidential information subject to the provisions of this clause, the Contractor should obtain a written determination from the Contracting Officer prior to any release, disclosure, dissemination, or publication.

(f) Contracting Officer determinations will reflect the result of internal coordination with appropriate program and legal officials.

(g) The provisions of paragraph (d) of this clause shall not apply to conflicting or overlapping provisions in other Federal, State, or local laws.

(End of clause)

Source: HHS.

Note: Effective January 2010, HHS has removed this clause from the HHSAR.

Appendix IV: Contractor Employee Nondisclosure Agreements Used by Agencies

Our review of the Department of Defense (DOD) and the Department of Homeland Security (DHS) contract clauses and provisions to protect sensitive information identified examples of standard nondisclosure agreement forms in use by these agencies consistent with internal control standards that call for restrictions on access to and accountability for resources and records.

Air Force Source Selection Non- disclosure Agreement

The Air Force Federal Acquisition Regulation Supplement (AFFARS) section on procurement integrity states that any individuals requiring access to source-selection information as a result of participating on a source selection or to perform their duties shall sign a Source Selection Non-disclosure Agreement identified in the Air Force mandatory procedure for source selection, and shown in figure 4.¹ The Source Selection Non-disclosure Agreement may be used on an annual basis for individuals who must have access to source-selection information in the performance of their official duties throughout the year, whether or not they participate as part of the actual source-selection team.

¹AFFARS Section 5303.104.

Appendix IV: Contractor Employee
Nondisclosure Agreements Used by Agencies

Figure 4: Source Selection Non-disclosure Agreement Used by the Air Force

SOURCE SELECTION NON-DISCLOSURE AGREEMENT	
Name: _____	Grade: _____
Job Title: _____	Organization: _____
Source Selection: _____ (or title of position, if used as an Annual Certificate IAW AFFARS 5303.104-4 .)	
Date: _____	
Briefing Acknowledgment	
<p>1. I acknowledge I have been assigned to the source selection (or position) indicated above. I am aware that unauthorized disclosure of source selection or proprietary information could damage the integrity of this procurement and that the transmission or revelation of such information to unauthorized persons could subject me to prosecution under the Procurement Integrity Laws or under other applicable laws.</p> <p>2. I do solemnly swear or affirm that I will not divulge, publish, or reveal by word, conduct, or any other means, such information or knowledge, except as necessary to do so in the performance of my official duties related to this source selection and in accordance with the laws of the United States, unless specifically authorized in writing in each and every case by a duly authorized representative of the United States Government. I take this obligation freely, without any mental reservation or purpose of evasion and in the absence of duress.</p> <p>3. I acknowledge that the information I receive will be given only to persons specifically granted access to the source selection information and may not be further divulged without specific prior written approval from an authorized individual.</p> <p>4. If, at any time during the source selection process, my participation might result in a real, apparent, possible, or potential conflict of interest, I will immediately report the circumstances to the Source Selection Authority.</p> <p>5. All personnel are requested to check the applicable block:</p> <p><input type="checkbox"/> I have submitted a current OGE Form 450, Executive Branch Confidential Financial Disclosure Report, as required by DODD 5500.07, Standards of Conduct.</p> <p><input type="checkbox"/> I am not required to submit an OGE Form 450.</p> <p><input type="checkbox"/> I have submitted a current SF278, Executive Branch Confidential Financial Disclosure Report, as required by DODD 5500.07, Standards of Conduct</p> <p><input type="checkbox"/> I am not required to submit a Form SF278</p> <p>OR</p> <p><input type="checkbox"/> I am a non-government employee. I have signed a proprietary information non-disclosure agreement that has been included in the contract between my firm and the government that precludes me from divulging any proprietary data to which I may gain access during the evaluation of proposals.</p> <p>Neither I, nor anyone in my immediate family, have any financial interest in any company involved in this acquisition as either a prime contractor or as a subcontractor.</p> <p>SIGNATURE: _____ DATE: _____</p> <p>Debriefing Certificate</p> <p>I have been debriefed orally by _____ as to my obligation to protect all information to which I have had access during this source selection. I no longer have any material pertinent to this source selection in my possession except material that I have been authorized in writing to retain by the SSA. I will not discuss, communicate, transmit, or release any information orally, in writing, or by any other means to anyone after this date unless specifically authorized to do so by a duly authorized representative of the United States Government.</p> <p>SIGNATURE: _____ DATE: _____</p>	

Source: Air Force.

**TRICARE
Management Activity
Confidentiality
Agreement (Non-
Federal Employee)
and Non-disclosure
Agreement for
Contractor
Employees and
Subcontractors**

Contractor conflict-of-interest-related procedures under the Department of Defense (DOD) TRICARE Management Activity's guidance on preparing nonpurchased care acquisition packages include the application of standard nondisclosure and confidentiality agreements with contractor employees. This guidance states that when evaluating contractor proposals, any contractor employees providing administrative support into the source selection process are required to review, sign, and adhere to a standard confidentiality agreement, shown in figure 5, which outlines their responsibilities.

Figure 5: Confidentiality Agreement Used by DOD's TRICARE Management Activity for Contractor Employees Providing Administrative Support into the Source-Selection Process

CONFIDENTIALITY AGREEMENT (NON-FEDERAL EMPLOYEE)¹

As a non-federal employee with access to information to be used in the evaluation of proposals for (short title of TMA requirement): _____,
(hereafter referred to as "proposals") under Solicitation Number: _____,
issued by the Contracting Office, I acknowledge that my conduct is governed by the
Procurement Integrity Regulations found at 48 CFR or FAR Part 3.104. I also recognize that that
the Contractor Bid or Proposal Information and Source Selection Information, relative to the
TMA Procurements, may be subject to further restrictions under the Trade Secrets Act, 18
U.S.C. 1832, 18 U.S.C.1905 and the Privacy Act, 5 U.S.C. 552a.

By executing this Confidentiality Agreement I agree not to disclose any Contractor Bid or
Proposal Information or Source Selection Information, relative to the TMA Procurements,
outside the federal government. I further agree that I will only disclose, within the federal
government, any Contractor Bid or Proposal Information or Source Selection Information,
relative to the TMA Procurements, to persons authorized to receive such information, in
accordance with applicable agency regulations or procedures. I also agree not to reproduce any
Contractor Bid or Proposal Information or Source Selection Information relative to the TMA
Procurements, except as authorized by the contracting officer or his or her authorized
representative. I also agree that, if I am requested to do so by the contracting officer, or his or
her authorized representative, I will promptly return, to the contracting officer, or to his or her
authorized representative, all Contractor Bid or Proposal Information or Source Selection
Information, relative to the TMA Procurements, that are in my possession. I also will promptly
return all copies of those materials that are in my possession.

By executing this Confidentiality Agreement I agree that, in the course of performing my duties
in the evaluation of proposals under the TMA Procurements, I will not use my position, or any
information contained in the Contractor Bid or Proposal Information or Source Selection
Information, relative to the TMA Procurements, to further my own private interest, to further my
business interest, or to further the private or business interests of another person or entity,
whether through advice, recommendation or by knowing of unauthorized disclosure of
information contained in the Contractor Bid or Proposal Information or Source Selection
Information. I understand the requirements of DoD 5500.7-R, Joint Ethics Regulation, Chapter
5, Conflicts of Interest. To the best of my knowledge, neither I nor any members of my
immediate family have a direct or indirect interest in any of the firms submitting a proposal for
the consideration of the evaluation panel which conflict substantially, or appear to conflict
substantially, with my duties in support thereof. I agree that, if in the course of performing my
duties in the evaluation of proposals under the TMA Procurements, I become aware that my
continued evaluation of proposals would conflict with my own private interest, my business
interest, or the private or business interests of an immediate family member, I will notify the
contracting activity immediately in writing and recuse myself from further evaluation of
proposals under the TMA Procurements.

¹ Executed in accordance with the requirements contained under 48 CFR 15.207(b)

**Appendix IV: Contractor Employee
Nondisclosure Agreements Used by Agencies**

(Continued)

Further, if I become aware of actions by any other person working with the proposals whose personal conduct may be in violation of the prohibitions in this paragraph or FAR Part 3.104, I will immediately notify the TMA Office of General Counsel in writing of this possibility.

By executing this Confidentiality Agreement I recognize that I may also have access to trade secrets, proprietary information, technical data, or computer software submitted by offerors under the TMA Procurements. I agree to abide by any restrictive markings on any such trade secrets, proprietary information, technical data, or computer software. By executing this Confidentiality Agreement I also agree that, if I am requested to do so by the contracting officer, I will execute a separate Use and Non-Disclosure Agreement as prescribed under 48 CFR 227.7103-7 (c).

A copy of the Procurement Integrity Regulations found in FAR Part 3.104 has been provided for my review. I have read this Agreement carefully and my questions, if any, have been answered to my satisfaction.

Printed
name: _____

Signature: _____

Title: _____ Date: _____

Witness
Signature: _____

Source: TRICARE Management Activity.

In addition, the guidance states that contractors performing many types of contract services are required to execute a standard nondisclosure agreement, shown in figure 6. This includes contractors not involved in acquisition support, when working on an order requiring access to the data, code, or products of another contractor.

Figure 6: Non-disclosure Agreement for Contractor Employees and Subcontractors
Used by DOD's TRICARE Management Activity

**NON-DISCLOSURE AGREEMENT FOR CONTRACTOR
EMPLOYEES AND THEIR SUBCONTRACTORS**

I, _____, am an employee of or a subcontractor to
_____(Company Name), a contractor acting under contract to the
_____(Name of TMA Directorate) under Prime Contract No. _____,
through Delivery Order _____.

I understand that in the performance of this task, I may have access to sensitive or proprietary business, technical, financial, and/or source selection information belonging to the Government or other contractors. Proprietary information includes, but is not limited to, cost/pricing data, Government spend plan data, contractor technical proposal data, independent government cost estimates, negotiation strategies and contractor data presented in negotiations, contracting plans, and statements of work. I agree not to discuss, divulge, or disclose any such information or data to any person or entity except those persons directly concerned with the performance of this delivery order. I have been advised that the unauthorized disclosure, use or negligent handling of the information by me could cause irreparable injury to the owner of the information. The injury could be source sensitive procurement information of the government or proprietary/trade secret information of another company.

As used in this agreement, sensitive information is an overarching term that includes, but is not limited to, sensitive but unclassified (SBU) information/data, Protected Health Information (PHI), For Official Use Only (FOUO), and Privacy Information (PI). This includes information in routine DoD payroll, finance, logistics, inventory, and personnel management systems. The loss of, misuse of, or unauthorized access to or modification of this information could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, as amended, but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.

I attest that I am familiar with, and I will comply with the standards for access, dissemination, handling, and safeguarding of the information to which I am granted access as cited in the Agreement and in accordance with the guidance provided to me relative to the specific category of information.

I understand that the United States Government may seek any remedy available to it to enforce this Agreement, including, but not limited to, application for a court order prohibiting disclosure of information in breach of this agreement. Court costs and reasonable attorney fees incurred by the United States Government may be assessed against me if I lose such action. I understand that another company might file a separate claim against me if I have misused its proprietary information.

(Continued)

Proprietary information/data will be handled in accordance with Government regulations. This agreement shall continue for a term of three (3) years from the date upon which I last have access to the information there from.

Sensitive information/data will be handled in accordance with Government regulations. The Statute of Limitation is indefinite for the unauthorized release of sensitive information.

In the event that I seek other employment, I will reveal to any prospective employer the continuing obligation in this agreement prior to accepting any employment offer.

The obligations imposed herein do not extend to information/data which:

- a) is in the public domain at the time of receipt, or it came into the public domain thereafter through no act of mine;
- b) is disclosed with the prior written approval of the TMA designated Contracting Officer;
- c) is demonstrated to have been developed by _____ (*Company Name*), or me independently of disclosures made hereunder;
- d) is disclosed pursuant to court order, after notification to the TMA designated Contracting Officer;
- e) is disclosed inadvertently despite the exercise of the same reasonable degree of care a party normally uses to protect its own proprietary information.

I have read this agreement carefully and my questions, if any, have been answered to my satisfaction.

(Printed Name of Employee or Subcontractor)

Date

(Signature of Employee or Subcontractor)

Organization

(Witness Signature)

Date

Source: TRICARE Management Activity.

DHS Non-disclosure Agreement

The DHS FAR supplement subpart relating to safeguarding classified and sensitive information within industry requires compliance with the policies and procedures in the agency management directive, which addresses safeguarding sensitive information originated within DHS in all contracts that involve contractor access to facilities, information

technology resources, or sensitive information.² Taken together, DHS's FAR supplement and security management directive require contractors and consultants with access to sensitive information to execute the DHS Form 11000-6, Sensitive But Unclassified Information Non-disclosure Agreement, shown in figure 7. According to the DHS security management directive, individual contractor employee execution of this nondisclosure agreement is a condition of access to such information. Additionally, to safeguard procurement integrity and personal conduct, DHS guidance states that government contractors who provide technical or other support services with respect to DHS source selections must complete this nondisclosure agreement.

²The Department of Homeland Security Acquisition Regulation (HSAR) Subpart 3004.470, *Safeguarding Classified and Sensitive Information within Industry* and DHS Management Directive System, *Safeguarding Sensitive But Unclassified (For Official Use Only) Information*, Management Directive (MD) No. 11042.1 (Washington, D.C.: Jan. 6, 2005).

Figure 7: DHS Form 11000-6, Sensitive But Unclassified Information Non-disclosure Agreement DHS Requires from Contractors and Consultants

DEPARTMENT OF HOMELAND SECURITY	
NON-DISCLOSURE AGREEMENT	
<p>I, _____, an individual official, employee, consultant, or subcontractor of or to _____ (the Authorized Entity), intending to be legally bound, hereby consent to the terms in this Agreement in consideration of my being granted conditional access to certain information, specified below, that is owned by, produced by, or in the possession of the United States Government.</p> <p>(Signer will acknowledge the category or categories of information that he or she may have access to, and the signer's willingness to comply with the standards for protection by placing his or her initials in front of the applicable category or categories.)</p>	
Initials:	Protected Critical Infrastructure Information (PCII)
<p>I attest that I am familiar with, and I will comply with all requirements of the PCII program set out in the Critical Infrastructure Information Act of 2002 (CII Act) (Title II, Subtitle B, of the Homeland Security Act of 2002, Public Law 107-296, 196 Stat. 2135, 6 USC 101 et seq.), as amended, the implementing regulations thereto (6 CFR Part 29), as amended, and the applicable PCII Procedures Manual, as amended, and with any such requirements that may be officially communicated to me by the PCII Program Manager or the PCII Program Manager's designee.</p>	
Initials:	Sensitive Security Information (SSI)
<p>I attest that I am familiar with, and I will comply with the standards for access, dissemination, handling, and safeguarding of SSI information as cited in this Agreement and in accordance with 49 CFR Part 1520, "Protection of Sensitive Security Information," "Policies and Procedures for Safeguarding and Control of SSI," as amended, and any supplementary guidance issued by an authorized official of the Department of Homeland Security.</p>	
Initials:	Other Sensitive but Unclassified (SBU)
<p>As used in this Agreement, sensitive but unclassified information is an over-arching term that covers any information, not otherwise indicated above, which the loss of, misuse of, or unauthorized access to or modification of could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, as amended, but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. This includes information categorized by DHS or other government agencies as: For Official Use Only (FOUO); Official Use Only (OUO); Sensitive Homeland Security Information (SHSI); Limited Official Use (LOU); Law Enforcement Sensitive (LES); Safeguarding Information (SGI); Unclassified Controlled Nuclear Information (UCNI); and any other identifier used by other government agencies to categorize information as sensitive but unclassified.</p> <p>I attest that I am familiar with, and I will comply with the standards for access, dissemination, handling, and safeguarding of the information to which I am granted access as cited in this Agreement and in accordance with the guidance provided to me relative to the specific category of information.</p>	
<p>I understand and agree to the following terms and conditions of my access to the information indicated above:</p> <ol style="list-style-type: none">1. I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of information to which I have been provided conditional access, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing this information have been approved for access to it, and that I understand these procedures.2. By being granted conditional access to the information indicated above, the United States Government has placed special confidence and trust in me and I am obligated to protect this information from unauthorized disclosure, in accordance with the terms of this Agreement and the laws, regulations, and directives applicable to the specific categories of information to which I am granted access.3. I attest that I understand my responsibilities and that I am familiar with and will comply with the standards for protecting such information that I may have access to in accordance with the terms of this Agreement and the laws, regulations, and/or directives applicable to the specific categories of information to which I am granted access. I understand that the United States Government may conduct inspections, at any time or place, for the purpose of ensuring compliance with the conditions for access, dissemination, handling and safeguarding information under this Agreement.	
DHS Form 11000-6 (08-04)	
Page 1	
Source: DHS.	

**Appendix IV: Contractor Employee
Nondisclosure Agreements Used by Agencies**

(Continued)

4. I will not disclose or release any information provided to me pursuant to this Agreement without proper authority or authorization. Should situations arise that warrant the disclosure or release of such information I will do so only under approved circumstances and in accordance with the laws, regulations, or directives applicable to the specific categories of information. I will honor and comply with any and all dissemination restrictions cited or verbally relayed to me by the proper authority.

5. (a) For PCII - (1) Upon the completion of my engagement as an employee, consultant, or subcontractor under the contract, or the completion of my work on the PCII Program, whichever occurs first, I will surrender promptly to the PCII Program Manager or his designee, or to the appropriate PCII officer, PCII of any type whatsoever that is in my possession.

(2) If the Authorized Entity is a United States Government contractor performing services in support of the PCII Program, I will not request, obtain, maintain, or use PCII unless the PCII Program Manager or Program Manager's designee has first made in writing, with respect to the contractor, the certification as provided for in Section 29.8(c) of the implementing regulations to the CII Act, as amended.

(b) For SSI and SBU - I hereby agree that material which I have in my possession and containing information covered by this Agreement, will be handled and safeguarded in a manner that affords sufficient protection to prevent the unauthorized disclosure of or inadvertent access to such information, consistent with the laws, regulations, or directives applicable to the specific categories of information. I agree that I shall return all information to which I have had access or which is in my possession 1) upon demand by an authorized individual; and/or 2) upon the conclusion of my duties, association, or support to DHS; and/or 3) upon the determination that my official duties do not require further access to such information.

6. I hereby agree that I will not alter or remove markings, which indicate a category of information or require specific handling instructions, from any material I may come in contact with, in the case of SSI or SBU, unless such alteration or removal is consistent with the requirements set forth in the laws, regulations, or directives applicable to the specific category of information or, in the case of PCII, unless such alteration or removal is authorized by the PCII Program Manager or the PCII Program Manager's designee. I agree that if I use information from a sensitive document or other medium, I will carry forward any markings or other required restrictions to derivative products, and will protect them in the same manner as the original.

7. I hereby agree that I shall promptly report to the appropriate official, in accordance with the guidance issued for the applicable category of information, any loss, theft, misuse, misplacement, unauthorized disclosure, or other security violation, I have knowledge of and whether or not I am personally involved. I also understand that my anonymity will be kept to the extent possible when reporting security violations.

8. If I violate the terms and conditions of this Agreement, such violation may result in the cancellation of my conditional access to the information covered by this Agreement. This may serve as a basis for denying me conditional access to other types of information, to include classified national security information.

9. (a) With respect to SSI and SBU, I hereby assign to the United States Government all royalties, remunerations, and emoluments that have resulted, will result, or may result from any disclosure, publication, or revelation of the information not consistent with the terms of this Agreement.

(b) With respect to PCII I hereby assign to the entity owning the PCII and the United States Government, all royalties, remunerations, and emoluments that have resulted, will result, or may result from any disclosure, publication, or revelation of PCII not consistent with the terms of this Agreement.

10. This Agreement is made and intended for the benefit of the United States Government and may be enforced by the United States Government or the Authorized Entity. By granting me conditional access to information in this context, the United States Government and, with respect to PCII, the Authorized Entity, may seek any remedy available to it to enforce this Agreement including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement. I understand that if I violate the terms and conditions of this Agreement, I could be subjected to administrative, disciplinary, civil, or criminal action, as appropriate, under the laws, regulations, or directives applicable to the category of information involved and neither the United States Government nor the Authorized Entity have waived any statutory or common law evidentiary privileges or protections that they may assert in any administrative or court proceeding to protect any sensitive information to which I have been given conditional access under the terms of this Agreement.

**Appendix IV: Contractor Employee
Nondisclosure Agreements Used by Agencies**

(Continued)

11. Unless and until I am released in writing by an authorized representative of the Department of Homeland Security (if permissible for the particular category of information), I understand that all conditions and obligations imposed upon me by this Agreement apply during the time that I am granted conditional access, and at all times thereafter.
12. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions shall remain in full force and effect.
13. My execution of this Agreement shall not nullify or affect in any manner any other secrecy or non-disclosure Agreement which I have executed or may execute with the United States Government or any of its departments or agencies.
14. These restrictions are consistent with and do not supersede, conflict with, or otherwise alter the employee obligations, rights, or liabilities created by Executive Order No. 12958, as amended; Section 7211 of Title 5, United States Code (governing disclosures to Congress); Section 1034 of Title 10, United States Code, as amended by the Military Whistleblower Protection Act (governing disclosure to Congress by members of the military); Section 2302(b)(8) of Title 5, United States Code, as amended by the Whistleblower Protection Act (governing disclosures of illegality, waste, fraud, abuse or public health or safety threats); the Intelligence Identities Protection Act of 1982 (50 USC 421 et seq.) (governing disclosures that could expose confidential Government agents); and the statutes which protect against disclosure that may compromise the national security, including Sections 641, 793, 794, 798, and 952 of Title 18, United States Code, and Section 4(b) of the Subversive Activities Act of 1950 (50 USC 783(b)). The definitions, requirements, obligations, rights, sanctions, and liabilities created by said Executive Order and listed statutes are incorporated into this agreement and are controlling.
15. Signing this Agreement does not bar disclosures to Congress or to an authorized official of an executive agency or the Department of Justice that are essential to reporting a substantial violation of law.
16. I represent and warrant that I have the authority to enter into this Agreement.
17. I have read this Agreement carefully and my questions, if any, have been answered. I acknowledge that the briefing officer has made available to me any laws, regulations, or directives referenced in this document so that I may read them at this time, if I so choose.

**DEPARTMENT OF HOMELAND SECURITY
NON-DISCLOSURE AGREEMENT
Acknowledgement**

Typed/Printed Name:	Government/Department/Agency/Business Address	Telephone Number:

I make this Agreement in good faith, without mental reservation or purpose of evasion.

Signature: _____ Date: _____

WITNESS:

Typed/Printed Name:	Government/Department/Agency/Business Address	Telephone Number:

Signature: _____ Date: _____

This form is not subject to the requirements of P.L. 104-13, "Paperwork Reduction Act of 1995" 44 USC, Chapter 35.

DHS Form 11000-6 (08-04)

Source: DHS.

Page 3

Department of the Treasury

The Department of the Treasury's (Treasury) reliance on private-sector resources to assist with implementing the Troubled Asset Relief Program (TARP) since its 2008 beginning underscores the importance of addressing conflict-of-interest issues. As we have previously reported, Treasury has strengthened its processes for managing and monitoring conflicts of interest among contractors and financial agents.³ In January 2009, Treasury issued an interim regulation on TARP conflicts of interest, which was effective immediately.⁴ Among other provisions, the regulation requires a certification, in the form of a nondisclosure agreement, from each retained entity's management official and key individuals performing work under a contract or financial agency agreement stating that he or she will comply with the requirements for confidentiality of nonpublic information before performing work and annually thereafter. An example of a nondisclosure agreement Treasury uses with its TARP contractors is shown in figure 8.

³GAO, *Troubled Asset Relief Program: One Year Later, Actions Are Needed to Address Remaining Transparency and Accountability Challenges*, [GAO-10-16](#) (Washington, D.C.: Oct. 8, 2009).

⁴TARP Conflicts of Interest, 74 Fed. Reg. 3431-3436 (Jan. 21, 2009) (codified at 31 C.F.R. Part 31).

Figure 8: Non-disclosure Agreement Used by the Department of the Treasury for TARP Contractor Employees and Management Officials

<p style="text-align: center;">NON-DISCLOSURE AGREEMENT</p> <p style="text-align: center;">Conditional Access to Nonpublic Information</p> <p>I, _____, employee of _____ (Organization) hereby consent to the terms in this Agreement in consideration of my being granted conditional access to certain United States Government nonpublic information.</p> <p>I understand and agree to the following terms and conditions:</p> <ol style="list-style-type: none">1. By being granted conditional access to nonpublic information, the _____ (Organization) and the U.S. Department of the Treasury (Treasury) have placed special confidence and trust in me, and I am obligated to protect this information from unauthorized disclosure, according to the terms of this Agreement.2. Nonpublic information refers to any information provided to me by the Treasury or _____ (Organization) in connection with my authorized services to the Treasury, or that I obtain or develop in providing authorized services to the Treasury, other than information designated as publicly available by the Treasury in writing or that becomes publicly available from a source other than the Financial Agent. Nonpublic information includes but is not limited to information about the Treasury's business, economic, and policy plans, financial information, trade secrets, information subject to the Privacy Act, personally identifiable information (PII), and sensitive but unclassified (SBU) information.3. PII includes, but is not limited to, information pertaining to an individual's education, bank accounts, financial transactions, medical history, and criminal or employment history and other information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual. This definition includes information that the loss, misuse, or unauthorized access to or modification of could adversely affect the privacy that individuals are entitled to under the Privacy Act.4. SBU information is any information where the loss, misuse, or unauthorized access to or modification of could adversely affect the national interest or the conduct of Federal programs. This definition includes trade secret or other information protected under the Trade Secrets Act, and may include other information designated by the Treasury or as defined by other Federal Government sources.5. I am being granted conditional access to nonpublic information, contingent upon my execution of this Agreement, to provide authorized services to the Treasury.

(Continued)

6. Except as set forth in paragraph 14 below, I shall never divulge any nonpublic information provided to me pursuant to this Agreement to anyone, unless I have been advised in writing by the _____ (Organization) and/or the Treasury that an individual is authorized to receive it.
7. I will submit to the Treasury for security review, prior to any submission for publication, any book, article, column or other written work for general publication that is based upon any knowledge I obtain during the course of my work in connection with the Treasury. I hereby assign to the Federal Government all rights, royalties, remunerations and emoluments that have resulted or will result or may result from any disclosure, publication, or revelation of nonpublic information not consistent with the terms of this Agreement.
8. If I violate the terms and conditions of this Agreement, I understand that the unauthorized disclosure of nonpublic information could compromise the security of individuals, the _____ (Organization) and the Treasury.
9. If I violate the terms and conditions of this Agreement, such violation may result in the cancellation of my conditional access to nonpublic information. Further, violation of the terms and conditions of this Agreement may result in the _____ (Organization) and/or the United States taking administrative, civil or any other appropriate relief.
10. I understand that the willful disclosure of information to which I have agreed herein not to divulge may also constitute a criminal offense.
11. Unless I am provided a written release by the Treasury from this Agreement, or any portions of it, all conditions and obligations contained in this Agreement apply both during my period of conditional access, and at which time and after my affiliation and/or employment with the _____ (Organization) ends.
12. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions shall remain in full force and effect.
13. I understand that the Treasury may seek any remedy available to it to enforce this Agreement, including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement.
14. I understand that if I am under U.S. Congressional or judicial subpoena, I may be required by law to release information, and that pursuant to 31 CFR Part 31, I shall provide prior notice to Treasury of any such disclosure or release.

I make this Agreement in good faith, without mental reservation or purpose of evasion.

Signature

Date

Source: Treasury.

Appendix V: Recent FAR Changes to Add Guidance and Contract Provisions for Information Technology (IT) Security

Between 2005 and 2007, contractor information-security and personnel-security requirements in the Federal Acquisition Regulation (FAR) were revised to assist agencies in reducing identified risks from contractors' access to sensitive federal facilities and information technology (IT) systems.

Federal Information-Security Oversight of Contractor IT Operations

Our April 2005 report concerning the federal government's extensive reliance on contractors to provide IT systems and services found that without appropriate policies and guidance on how to develop effective information-security oversight of contractors, agencies may not develop sufficient policies to address the range of risks posed by contractors, and that as a result, federal information and operations can be placed at undue risk.¹ Since FAR Council efforts to update the FAR provisions had stretched over 3 years, we recommended expeditious completion to ensure that agencies develop appropriate information-security oversight capabilities.

Five months later, in September 2005, an interim rule amending the FAR was published.² In implementing the IT security provisions of the Federal Information Security Management Act of 2002 (FISMA), the FAR Council stated that the interim rule change was necessary to ensure the government was not exposed to inappropriate and unknown risk. Unauthorized disclosure, theft, or denial of IT resources had the potential to disrupt agency operations and could have financial, legal, human safety, personal privacy, and public confidence effects, according to the FAR Council. Adding specific FISMA-related provisions was intended to provide clear, consistent guidance to acquisition officials and program

¹GAO, *Information Security: Improving Oversight of Access to Federal Systems and Data by Contractors Can Reduce Risk*, [GAO-05-362](#) (Washington, D.C.: Apr. 22, 2005). The IT systems and services provided by contractors include computer and telecommunication systems and services, as well as the testing, quality control, installation, and operation of computer equipment. Additionally, contractors provide services and systems on behalf of agencies at contractor facilities or to an agency via remote access. We found that the methods that agencies were using to ensure information security oversight of contractor operations had limitations and needed strengthening. For example, most agencies had not incorporated the Federal Information Security Management Act of 2002 (FISMA) requirements, such as annual testing of controls, into their contract language. Few agencies had established specific information-security oversight policies for contractor IT operations.

²Interim Rule, FAR Case 2004-018, *Information Technology Security*, 70 Fed. Reg. 57449-52, (Sept. 30, 2005). A year later, after consideration of public comments, the interim rule was adopted without change.

managers, and to encourage and strengthen communication with IT security officials, chief information officers, and other affected parties. Among other changes this rule amended the FAR by

- adding a definition for the term “Information Security” to FAR Subpart 2.1, as shown in the text box below;
- incorporating IT security requirements in acquisition planning and when describing agency needs; and
- revising the policy in FAR Subpart 39.101 for IT acquisitions to require including the appropriate agency security policy and requirements.

FAR Subpart 2.1 Definition of Information Security Added in 2005

Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide—

1. Integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;
2. Confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and
3. Availability, which means ensuring timely and reliable access to, and use of, information.

Source: 70 Fed. Reg. 57449-52 (Sept. 30, 2005).

Personal Identity Verification of Contractor Personnel

In 2007 the FAR was amended to add personnel-security requirements, in recognition that contractors increasingly are required to have physical access to federally controlled facilities and information systems in the performance of government contracts and the President’s issuance of Homeland Security Presidential Directive 12 (HSPD-12). Specifically, the FAR was amended to require agencies to include a standard clause in their solicitations and contracts when contractor performance requires recurring access to government facilities and systems. This clause states that the contractors shall comply with agency personal identity verification procedures for issuance of identification cards.³ This action to unify FAR guidance has assisted agencies in implementing HSPD-12, requiring the establishment of a governmentwide standard for secure and reliable forms of identification cards for federal employees and

³Final Rule, FAR Case 2005-017, *Requirement to Purchase Approved Authentication Products and Services*, amended FAR Subpart 4.13 and 52.204-9. 72 Fed. Reg. 46333-35 (Aug. 17, 2007).

contractors alike. For example, updates issued since 2007 to some agency FAR supplements have added agency-specific HSPD-12 policies, procedures, contract clauses, and solicitation provisions for contractor employees requiring routine access to their facilities and sensitive information stored in agency networks.⁴

Implementing HSPD-12 requirements through contract provisions helps address the risks of contractors gaining unauthorized physical or electronic access to federal information or contractors using outmoded identification cards that can be easily forged, stolen, or altered to allow unauthorized access. In 2009 the FAR Council opened a FAR case in recognition of the need for return of the physical identification cards issued to contractors.⁵ According to the FAR Council, our review of contractor employees' access to sensitive information reinforced the need to resolve this shortcoming in FAR guidance.

⁴For example, effective January 26, 2010, the Department of Health and Human Services (HHS) revised its FAR supplement to reflect FAR policy and other changes since the last update in December 2006. A new Subpart 304.13, *Personal Identity Verification*, was added with new policy to implement HSPD-12 in HHS. The HHS implementation includes applicable solicitation provisions and contract clauses to provide a consistent and systematic approach to ensure the security of HHS facilities and information systems. 74 Fed. Reg. 62396-97 (Nov. 27, 2009).

⁵FAR case number 2009-027—Personal Identity Verification of Contractor Personnel. The proposed rule for this case was published in the Federal Register for public comment. 75 Fed. Reg. 28771 (May 24, 2010). The proposed rule seeks to provide additional regulatory coverage in FAR Subpart 4.13 and clause 52.204-9 to reinforce the requirement of collecting from contractors all forms of government-provided identification once they are no longer needed to support a contract. Public comments were due July 23, 2010.

Appendix VI: Comments from the Department of Homeland Security

Note: Page numbers in the draft report may differ from those in this report.

U.S. Department of Homeland Security
Washington, DC 20528



**Homeland
Security**

September 1, 2010

Mr. John Needham
Director, Acquisition and Sourcing Management
Government Accountability Office
Washington, DC 20548

Dear Mr. Needham:

Thank you for the opportunity to comment on the draft report GAO-10-693 "Contractor Integrity: Stronger Safeguards Needed for Contractor Access to Sensitive Information."

While DHS generally concurs with the contents of the GAO draft report, we take exception to Table 3 on Page 16 of the draft report and one comment on Page 17 of that report.

As noted in the draft report, GAO analyzed a total of 42 contracts government-wide, including 14 DHS contracts. The GAO report asserts that three of these 14 DHS contracts lacked the necessary safeguards (per Table 3 of the draft report). The DHS Office of the Chief Procurement Officer (OCPO) believes that one of these three DHS contract actions contains adequate safeguards. Specific details for this contract action are provided below:

- **HSQDC-06-J-00191, Systems Research and Applications Corp. (SRA)**, executed on July 3, 2006, is for support services for planning, implementing, and monitoring privacy regulations and guidelines. While the task order does not contain HSAR 3052.204-71, it does effectively contain the same language as HSAR 3052.204-71. The contract includes the following four requirements:
 - "(c) Contractor employees working on this contract must complete such forms as may be necessary for security or other reasons, including the conduct of background investigations to determine suitability."
 - "(d) The Contracting Officer may require the contractor to prohibit individuals from working on the contract if the government deems their initial or continued employment contrary to the public interest for any reason..."
 - "(e) ... the Contractor shall not disclose, orally or in writing, any sensitive information to any person unless authorized in writing by the Contracting Officer. For those contractor employees authorized access to sensitive information, the contractor shall ensure that these persons receive training concerning the protection and disclosure of sensitive information both during and after contract performance."

- 2 -

- “(f) The Contractor shall include the substance of this clause in all subcontracts at any tier where the subcontractor may have access to Government facilities, sensitive information, or resources.”

(paragraphs (a) and (b) consist of definitions)

The following identifies language in the section of the task order titled “Security Requirements” that is comparable to the four requirements in HSAR 3052.204-71 (“Security Requirements” are on pages 5-10 of the statement of work (SOW) – the task order pages are unnumbered):

- Comparable to HSAR 3052.204-71(c): “Contract employees (to include applicants, temporaries, part-time and replacement employees) under the contract, needing access to sensitive information, shall undergo a position sensitivity analysis based on the duties each individual will perform on the contract. The results of the position sensitivity analysis shall identify the appropriate background investigation to be conducted. All background investigations will be processed through the Security Office. Prospective Contractor employees shall submit the following completed forms to the Security Office through the COTR no more than two (2) weeks after, whether a replacement, addition, subcontractor employee, or vendor:
 1. Standard Form 85P, ‘Questionnaire for Public Trust Positions’
 2. FD Form 258, ‘Fingerprint Card’ (2 copies)
 3. Conditional Access to Sensitive But Unclassified Information Non-Disclosure Agreement
 4. Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act” (page 7 of the SOW).
- Comparable to HSAR 3052.204-71(d): “DHS reserves the right and prerogative to deny and/or restrict the facility and information access of any Contractor employee whom DHS determines to present a risk of compromising sensitive Government information to which he or she would have access under this contract.” (page 6 of the SOW).
- Comparable to HSAR 3052.204-71(e): Several portions of the SOW address disclosure and training:
 1. The requirement in HSAR 3052.204-71(c) that contractor and subcontractor employees complete the “Conditional Access to Sensitive But Unclassified Information Non-Disclosure Agreement” (see above)
 2. “When sensitive government information is processed on Department telecommunications and automated information systems, the Contractor agrees to provide for the administrative control of sensitive data being processed and to adhere to the procedures governing such data as outlined in DHS IT Security Program Publication DHS MD 4300.1” (page 9 of the SOW, under “Information Technology Security Clearance”).
 3. “Contractors, who are involved in management, use, or operation of any IT systems that handle sensitive information within or under the supervision of the Department, shall receive periodic training at least annually in security awareness and accepted security practices and systems rules of behavior. Department contractors, with significant security operations, shall receive specialized training specific to their security responsibilities annually” (page 9 of the SOW, under “Information Technology Security Training and Oversight”).

- 3 -

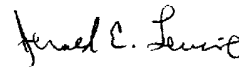
- o Comparable to HSAR 3052.204-71(f): Several portions of the SOW address the flow-down of requirements to subcontractors:
 1. Page 7 of the SOW requires each subcontractor employee to submit four forms (see above).
 2. "Some material will contain proprietary, sensitive, or classified data from various public or private sources. The contractor shall require all subcontractors to sign corporate and individual non-disclosure agreements" (page 10 of the SOW, under "Other Pertinent Information or Special Considerations").
 3. "The Contractor shall ensure that each of its employees, consultants, and subcontractors who work on the PCII [Protected Critical Infrastructure Information] Program have executed Non-Disclosure Agreements (NDAs) in a form prescribed by the PCII Program Manager. The Contractor shall ensure that each of its employees, consultants and subcontractors has executed a NDA and agrees that none of its employees, consultants or subcontractors will be given access to Protected CII without having previously executed a NDA" (page 10 of the SOW, under "Non-Disclosure of Protected Critical Infrastructure Information").

Therefore, DHS OCPO believes that although HSHQDC-06-J-00191 does not contain HSAR 3052.204-71, it does contain comparable and adequate language.

In addition, on Page 17, the second sentence of the first complete paragraph states that: "For example, three DHS task orders of the 14 contract actions reviewed did not include the contract clause required when contractors need recurring access to government facilities or sensitive information." In accordance with the DHS OCPO comments provided above regarding page 16, table 3, we believe that the SRA task order, which is included as one of the three DHS task orders noted as deficient within this sentence, actually does contain adequate contract language with respect to contractor access to sensitive information.

Thank you again for the opportunity to provide comments on the draft report.

Sincerely,



Jerald E. Levine
Director
Departmental GAO/OIG Liaison Office

Appendix VII: GAO Contact and Staff Acknowledgments

GAO Contact

John K. Needham, (202) 512-4841 or needhamjk1@gao.gov

Staff Acknowledgments

In addition to the contact named above, Carolyn Kirby, Assistant Director; Jennifer Dougherty; Guisseli Reyes-Turnell; Greg Campbell; Vijay D'Souza; Claudia Dickey; Ralph Roffo; Tind Shepper Ryen; Alyssa Weir; and Bill Woods made key contributions to this report.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's Web site, <http://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm

E-mail: fraudnet@gao.gov

Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548